نقش بسیج مردمی در پدافند سایبری وتأثیر آن برامنیت ملی جمهوری اسلامی ایران

نویسنده: غلامرضا بیات[1]

تاریخ دریافت: ۹۱/۱۰/۱۷ تاریخ پذیرش نهایی: ۹۲/۲/۲۵

فصلنامه مطالعات راهبردی بسیج، سال شانزدهم، شماره ۵۸، بهار ۱۳۹۲

چکیده

جمع‌بندی حاصل از نظرات کارشناسان مربوط و یک دهه تجربهٔ محقق در فضای مجازی و بسیج مردمی، گویای آن است که با به کارگیری توان بسیج مردم در پدافند سایبری و فضای مجازی، می‌توان بر امنیت ملی تأثیر گذاشت؛ اما چگونگی این تأثیر، نیاز به پژوهشهایی دارد که تلاش محقق در این مقاله در راستای آن است. در این مقاله با بحث روی بسیج مردمی، پدافند سایبری و امنیت ملی به عنوان سه متغیّر موضوع مقاله، شاخصه‌های هر یک از این متغیّرها از جمع‌بندی نظرات کارشناسان و گردآوری میدانی داده‌ها و مشاهدات و تجربیات نویسنده، احصا شده و داده‌های گرد آوری شده مورد تجزیه و تحلیل قرار گرفتند. نتایج تحقیق نشان می‌دهد که بر اساسِ تغییرِ مناسب در راستای تقویت شاخصه‌های احصا شده، می‌توان با بهره‌گیری از توان بسیج مردمی و فنون پدافندسایبری در جهت ارتقای سطح امنیت ملی گامهای مؤثری برداشت. در پایان کار، با توجه به تجزیه و تحلیل داده‌ها، مشاهدات محقق و نظرات متخصصان امر، یافته‌ها و نتایج به دست آمده از تحقیق ارائه شده است.

واژگان کلیدی:

بسیج مردمی، فضای مجازی، پدافند سایبری، امنیت ملی

---

۱. کارشناس ارشد اطلاعات راهبردی دانشگاه جامع امام حسین(ع). Bayat@mailfa.org

مقدمه

حفظ امنیت ملی، هدف غایی و اساس اقدامات اکثر دولتها، کشورها و واحدهای سیاسی امروز است (ویکی‌پدیا، ۱۳۹۲) و در نظام جمهوری اسلامی ایران، آرمانها، اهداف غایی و ارزشهای اصلی، شاملِ پاسداری از انقلاب اسلامی، حفظ نظام و حراست از دستاوردهای انقلاب اسلامی است. از آنجا که امام خمینی(ره) بنیانگذار انقلاب اسلامی ایران فرمودند: «حفظ نظام جمهوری اسلامی از اوجب واجبات است حتی از نماز هم واجب‌تر است»(وبگاه امام خمینی)؛ از این رو، امنیت ملی، هدف واسطی است که در چارچوب حراست از انقلاب اسلامی و دستاوردهای آن و حفظ کیان نظام اسلامی تعریف می‌شود. بنابراین، امنیت ملی در طول حفظ نظام اسلامی و نه در عرض آن است. امنیت ملی، ممکن است در ابعاد نظامی، سیاسی، اقتصادی، فرهنگی، اجتماعی، صنعتی و سایبری، مورد تهدید قرار گیرد.(بیات، ۱۳۹۱)

فضای سایبر عرصه‌ای است که امروزه در طراحی‌های عملیات روانی و ساماندهی شبکه‌های اجتماعی مجازی برای ایجاد و مدیریتِ شورش و بحران، تأثیرگذاری بر افکار عمومی و امنیت ملی کاربرد مؤثر دارد؛ به طوری که نمی‌توان و نمی‌شود نقش فنّاوری اطلاعات و ارتباطات در فضای مجازی و تأثیر بالفعل و بالقوّهٔ آن را در نبردهای اطلاعاتی نادیده گرفت. فضای مجازی و اینترنت، تفاوت زیادی به زندگی مردمِ سراسر جهان داده است؛ برای نمونه، حوادث اخیر کشورهای عربی نشان داد اینترنت و رسانه‌های اجتماعی می‌توانند در ارتقای توانایی و تأثیرجوانان و زنانِ به حاشیه رانده شده، نقش حیاتی داشته باشند.(اشتون،[1] ۲۰۱۳: ۸)

در ناآرامی‌های پس از انتخابات ریاست جمهوری ایران در سال ۱۳۸۸ شاهد بودیم رئیس جمهور آمریکا به شرکت تویتر دستور داد برای استفاده از ظرفیت فضای مجازی و شبکه‌های اجتماعی در بهره‌گیری علیه اوضاع داخلی ایران، این شرکت مدتی تعمیرات داخلی خود را متوقف کند تا ارتباط کاربران اینترنت در ایران با مشکل مواجه نشود. دولت ایران نیز با محدود کردن دسترسی به اینترنت و فیلتر کردن تویتر و فیس‌بوک در آن مقطع زمانی، بر فضای مجازی داخل کشور تسلّط نسبی یافت و برناآرامی‌ها چیره شد. گروههای خودجوش مردم ایران نیز با حمایتهای خود ازنظام حاکم بر ایران در فضای مجازی و با سایر فنون پدافندی، از اثرات آفندی دشمن و عملیات روانی و شبکه‌سازی او علیه ایران در فضای مجازی کاستند. طی این غائله، در فضای مجازی (اینترنت و ماهواره) تبلیغات وسیعی علیه نظام جمهوری اسلامی به راه انداخته شد و جمع قابل ملاحظه‌ای به میدان آمد و

1. Ashton

موضوع امنیت ملی ایران به چالش کشیده شد. حتی دشمن در وبگاههایی نحوهٔ ساخت سلاحهای دست‌ساز و بمبهای تروریستی را آموزش می‌داد که این سایتها توسط گروهها و افراد داوطلب مردمی وفادار به نظام، شناسایی و جهت مقابلهٔ سایبری به حاکمیت معرفی شدند و دستگاههای اجرایی نیزبا فنونی نظیر ۹ دی و مقابله با این وبگاهها، موضوع رامدیریت کرد.

بدین ترتیب، درآفند و پدافند سایبری، نقش مردم و بسیج مردمی را نمی‌توان نادیده گرفت و بسیج مردمی همانند فضای واقعی، درفضای مجازی هم نقش و نمود پیدا می‌کند. اینترنت، شبکه‌های ماهواره‌ای و فضای مجازی، امروزه ابزار کارامد اطلاع‌رسانی بوده، تأثیر زیادی درکنش و واکنشهای اجتماعی و فرهنگی جوامع دارد؛ به طوریکه جنگ سایبری و فعالیت درفضای مجازی، از ابزارعملیات روانی و تهاجم فرهنگی کشورها علیه رقیب، دشمن و حریف بوده، برای ایجاد اغتشاش و بحران و تأثیرگذاری برافکار عمومی و امنیت ملی، کاربرد مؤثر دارد.

امروزه اهمیت فضای مجازی به حدّی است که برخی نظریه‌پردازان، قدرت سایبری را بُعد پنجم قدرت بعد از ابعاد زمینی، دریایی، هوایی و فضایی می‌دانند(نای، ۱۳۸۷: ۹). فضای مجازی، اینترنت وشبکه‌های ماهواره‌ای،امروزه ابزاری برای کاربردی وعملیاتی کردن اطلاعات راهبردی وتاکتیکی و برنامه‌های عملیات روانی و فرهنگی است. در وقایع اخیر کشورهای شمال آفریقا شاهدیم گروهی از جوانان تونسی در شبکه‌های اجتماعی مجازی تصمیم به اعتراض و تظاهرات می‌گیرند ودرظرف کمتر از یک ماه، نه تنها بالاترین رئیس اجرایی کشورشان را فراری می‌دهند، بلکه جرقهٔ آتش حرکتهای مشابه در سایر کشورهای منطقه می‌شوند.تأثیر فضای مجازی در سازماندهی وبه ثمر نشاندن این حرکات اجتماعی وسیاسی، برکسی پوشیده نیست و اینکه یک مرد مصری نام دختر تازه متولد شدهٔ خود را فیس‌بوک[1] بگذارد، تعجب‌انگیز نخواهد بود(بیات، ۱۳۹۱: ۳۰۰). ایران نیز درمعرض هجمه‌ها و شبیخون سایبری دشمنان قراردارد و افزایش سطح امنیت ملی آن، نیاز به حرکت هوشمندانه درعرصهٔ دفاع سایبری داردکه دراین میان، نقش بسیج مردمی و ورود شبکه‌های اجتماعی مجازی به عرصهٔ دفاع سایبری، حائز اهمیت است.

باتوضیحات پیش‌گفته،چه زمینه‌هایی وجودداشته که اقدامات دشمن درفضای مجازی برای سازماندهی ناآرامی‌ها علیه امنیت ملی ایران مؤثر واقع افتاد؟ به نظر می‌رسد برای مقابله با آن شرایط، راهکار استفاده ازبسیج مردمی و پدافندسایبری در ارتقای سطح امنیت ملی ایران می‌تواند مؤثرباشد.

1. Facebook

با توجه به تجربیات کاری پژوهشگر که بیش از یک دهه در فضای مجازی و سایبری به طور حقیقی و حقوقی فعال بوده و از نزدیک با مشکلات آن آشنایی نسبی دارد، دریافته است که با مدیریت فضای مجازی و شبکه‌های اجتماعی مجازی مردمی و با به کارگیری بسیج مردمی و تقویت پدافند سایبری می‌توان بر امنیت ملی تأثیر داشت؛ اما چگونگی آن، نیاز به انجام پژوهشهایی دارد که در این پژوهش تلاش شده این مهم انجام شود؛ هرچند در تجزیه وتحلیلِ مسائلِ امنیتِ سایبری، به دلیل عدم توافق برواژگان واستفاده اززبان اغراق‌آمیز، معمولاً نتیجه تضعیف می‌شود.(سومرو براون[1]، ۲۰۱۱: ۲۷)

صاحب‌نظران و متخصصان پدافند سایبری، بسیج مردمی و امنیت ملی، در سازمانها و مراکز مختلف (سازمان بسیج مستضعفین، سازمان پدافند غیر عامل، دانشکده پدافند سایبری، پلیس فتا، فرماندهی سایبری سازمان اطلاعات سپاه و...)، همگی تأکید و اذعان بر لازم و مورد نیاز بودن انجام این تحقیق برای کشور داشتند که اهمیت و ضرورت تحقیق در خصوص موضوع این مقاله را دو چندان کرد و تعیین مؤلفه‌ها و شاخصه‌هایی از بسیج مردمی و پدافند سایبری که در امنیت ملی و پایداری آن مؤثر است، راهگشای برنامه‌ریزان دفاعی، امنیتی، اطلاعاتی و ارتباطی کشور می‌تواند باشد. هدف تحقیق، شناخت این موضوع است که چگونه می‌توان از طریق بسیج مردمی، پدافند سایبری را تقویت و باعث ارتقای سطح امنیت ملی ج.ا. ایران شد؟

سؤال تحقیق: بسیج مردمی چگونه می‌تواند در تقویت پدافند سایبری و از طریق آن در ارتقای سطح امنیت ملی جمهوری اسلامی ایران نقش داشته باشد؟

روش تحقیق

روش انجام تحقیق اصلی که این مقاله مستخرج از آن است، ترکیبی از روشهای تحقیق کمّی[2] و کیفی است و چون تأکید سؤال تحقیق روی «چگونگی»است، لذا روش انجام این تحقیق، تبیینی بوده و به صورت پیمایشی و با مطالعات میدانی و در سطح میانه (ملی) انجام شده است. بخشهایی نیز حاصلِ بیش از یک دهه تجربه، مشاهدات و تخصص محقق در فضای سایبر و مدیریت اموربسیج است.

جامعهٔ آماری شامل افرادی با تحصیلات تکمیلی(کارشناسی ارشد، دکترای حرفه‌ای و دکترای تخصصی) می‌باشد که در جمهوری اسلامی ایران ساکن و شاغل

1. Sommer & Brown
2. Quantitative Research

بوده، از فضای مجازی استفاده می‌کنند و آشنایی حداقلی با ویژگی‌های فضای سایبر دارند. جامعهٔ آماری ۱۱۷۳۸۰۰ نفر محاسبه و براساس فرمول کوکران بر روی حجم نمونهٔ ۲۰۵ نفر به اجرا درآمد.

ابزار گردآوری داده‌ها در تحقیق، پرسشنامهٔ پژوهشگر ساخته بوده وبرای طرح سؤال، از منابع موجود، نتایج بررسی آثار و به خصوص نظرات کارشناسان امر و تجربیات محقق استفاده شده است. پرسشنامه، شامل دو دسته سؤالات عمومی و تخصصی است؛ سؤالات عمومی، شامل مشخصات فردی پاسخ‌دهندگان از قبیل جنسیت، سن، مرتبهٔ سازمانی، وضعیت استخدامی، میزان تحصیلات، میزان مهارت در استفاده از اینترنت و... بوده وسؤالات تخصصی، براساس مؤلفه‌های تشکیل‌دهندهٔ موضوع مقاله، شکل گرفته است. سؤالات تخصصی پرسشنامه با توجه به سه متغیّره بودن موضوع مقاله، در سه بخش شامل ۳۰ سؤال،تقسیم و عملیاتی شده است(هر متغیّر ۱۰ سؤال). روایی[1] با اعتبار عاملی و پایایی[2] ابزار گردآوری داده‌ها و اطلاعات از روش آلفای کرونباخ استفاده شد که مقدار ضریب آلفای کرونباخ، توسط نرم افزار SPSS مقدار۰/۸۷۴ محاسبه شد و چون بزرگ‌تر از ۰/۷ است، لذا با توجه به تحلیل کرونباخ، پرسشنامه از پایایی قابل قبولی برخوردار است.[3]

مبانی مفهومی- نظری موضوع

بسیج مردمی

نیروی انسانی یک کشور، عنصر حیاتی و اصلی در «قدرت ملی» آن کشور است. از اینرو، حضرت امام خمینی(ره) «بسیج نیروهای مردمی» را در سطح ملی و جهانی همواره مورد تأکید قرار می‌دادند(مطهرنیا، ۱۳۷۶: ۳۷) و از بسیج به عنوان «پیشگامان رهایی» یاد می‌کردند(کیوان حسینی، ۱۳۸۱). موضوع بسیج از پدیده‌های اجتماعی است که منحصر به یک جامعهٔ ویژه با تفکری خاص نیست. هرچند هر جامعه‌ای بسیج را در چارچوب ایدئولوژی خاص خود تعریف و تحلیل می‌کند، اما شاخصه‌های کلی و مشترکی در توده‌ها و جوامع وجود دارد که می‌تواند سطوح مختلفی از بسیج را مطرح و ارائه کند(کلهر، ۱۳۸۶: ۶). بسیج به مثابهٔراهبرد بازدارندگی مردمی است و برای تحقق فضای مناسب دفاع فرهنگی، بسیج همهٔ منابع در هرسطحی ضرورت دارد.(کیوان حسینی، ۱۳۸۱)

1. Validity
2. Reliability

۳. خوانندگان محترم می‌توانند برای اخذ توضیحات بیشتر به اصل پایان‌نامه مراجعه کنند که در دانشگاه جامع امام حسین(ع) با نمره عالی دفاع شده است.

هر حکومتی برای جلوگیری از ستیزه‌جویی عناصر خارج از قدرت وافزایش قدرت متّکی بر توده‌ها، نیازمند بسیج است. مطمئن‌ترین واصلی‌ترین عنصر برای ایجاد نظم سیاسی وحفظ قدرت حاکمیت، بسیج است که به معنای دخیل کردن توده‌ها در فعالیتهای سیاسی از طریق بستر مناسب، مشروع و قابل کنترل است(مطهرنیا، ۱۳۷۶: ۲۶). کرونین با تأکید بر نقش مردم در بسیج عنوان می‌دارد: «بسیج توده‌ها عبارت است از تأمین تعداد زیادی سرباز مورد پشتیبانی مردم. ابزارها و اهداف بسیج عمومی در حال تغییرند و با رویکرد سنتی حکومت محور، تفاوت دارند. تحولات پویای اجتماعی، اقتصادی و سیاسی امروز به اندازهٔ تغییرات پایان قرن هجدهم میلادی، برای جنگ اهمیت دارند. مهم‌ترین آنها شیوهٔ نوین جذب نیرو در قرن۲۱ است. بسیج عمومی دارای یک شبکهٔ ارتباطی است که از فضای سایبرنتیک سرچشمه می‌گیرد و تأثیری مستقیم روی واقعیت مادی(بیرونی) دارد. شبکه‌های ارتباطی معمولی در دسترس افراد، مانند رایانه‌های شخصی، ماهیت تعامل اجتماعی انسانی را تغییر می‌دهند و بدین ترتیب، بر شکل و نتیجه منازعات بین‌المللی و داخلی هم تأثیر می‌گذارند»(کرونین، ۱۳۸۵: ۷۴). بسیج، بهترین پایگاهی است که می‌تواند کوششهای مشترک و توأمان مردمی و دولت را برای بهبود اوضاع اقتصادی، اجتماعی، فرهنگی و نظامی در هر محل هماهنگ کرده، مردم آن محل را در زندگی اجتماعی ترکیب کند و آنها را تماماً برای مشارکت در پیشرفت ملی توانا سازد(مطهرنیا، ۱۳۷۶: ۲۷). نقش مردم به عنوان مرجع و مهم‌ترین عامل تأمین امنیت از ارزش بسیاری برخوردار است که میزان آن به نسبت همراهی و همکاری مردم با حاکمیت محاسبه می‌شود(روحی، ۱۳۹۱: ۷۲). هر چند برخی نظیر رابینز[1] و وبستر[2] معتقدند سازوبرگ جنگ اطلاعاتی، برای پیشبرد امر جنگ، نه به بسیج شهروندان نیاز دارد و نه به بسیج صنایع(رابینز و وبستر، ۱۳۸۴: ۲۲۳)؛ اما باید گفت که امروزه، نه تنها سازوبرگ جنگ اطلاعاتی بی‌تأثیر از مردم و فنّاوری نیست، بلکه با شرایطی، مکمّل هم می‌توانند باشند. با این بیانِ وبستر و رابینز، مشخص می‌شود که منظور آنها از بسیج شهروندان، گسیل کردن نیروی نظامی و مردمی به جبههٔ جنگ سخت است که در این نوع جنگ لازم نیست؛ در حالیکه در جنگ و دفاع سایبری در فضای مجازی مردم و کاربرانِ اینترنت و فنّاوری‌های پیشرفته برای پیشبرد اهداف جنگ و دفاع بسیار مؤثرند که در طول این مقاله به مواردی اشاره می‌شود. البته ناگفته نماند رابینز و وبستر،تأثیرمردم را در انقلاب مدّ نظر دارند و عنوان می‌کنند: «برای انقلاب کردن، شما به مردم نیاز دارید».(همان: ۳۲۹)

1. Kevin Robbins
2. Frank Webster

در بحث امنیت ملی، نقش مردم و بسیج عمومی غیرقابل چشم‌پوشی است و می‌دانیم استفاده از ظرفیت و بسیج مردمی هم می‌تواند در دو نوع ذیل قابل بهره‌برداری باشد:

۱. حرکت خودجوشِ مردم برای انجام کاری که بیشتر از احساسات سرچشمه می‌گیرد و معمولاً کوتاه‌مدت است.

۲. حرکت برنامه‌ریزی شده و سازماندهی شدهٔ مردم برای نیل به یک هدف مشخص؛که نسبت به نوع اول دارای عقلانیت بیشتری بوده و شامل اهداف میان‌مدت یا بلندمدت‌تری است.(بیات، ۱۳۹۱: ۳۰۰)

هر دو روش مذکور در فضای مجازی و فضای واقعی نمود پیدا می‌کندکه منظور ما دراین مقاله، بیشتربر جنبهٔ فضای سایبری تأکید دارد. دراین مقاله، بسیج مردمی، استفاده از توان مردم درراستای رسیدن به اهداف یک گروه، سازمان یا دولت و به طورخاص ارتقای سطح امنیت ملی کشور خود یاتنزیل سطح امنیت ملی برای کشورحریف یادشمن تعریف می‌شودکه می‌تواند شامل هر دونوع ذکر شده برای بسیج مردمی باشد. بیشترمدّ نظر، روشها و اقداماتی مردمی است(مثلاً درشبکه‌های اجتماعی مجازی)که برپدافندسایبری تأثیر دارد؛ چه بسیج سازماندهی شده و چه حرکت خودجوش مردمی و به خصوص تأثیراتی که برامنیت ملی جمهوری اسلامی ایران می‌تواند اعمال کند.

جنگ و دفاع سایبری

تاریخچهٔ جنگ ودفاع سایبری به زمان ابداع رایانه برمی‌گردد(لیبیکی، ۱۳۸۴: ۵)؛ آنگاه که رایانه پدیدآمد و به تبعِ آن سایبر؛یعنی علم فرمان انسان به ماشین و رایانه(نرم‌افزار و سخت‌افزار) و مدیریت آن مطرح شدو روزبه روز درمفاهیم گسترده‌تری نظیربسیج سایبری،[1] تروریسم سایبری،[2] جنگ سایبری،[3] فرهنگ سایبری[4] و... خودنمایی کرد.آنجا که عده یاگروه یاکشوری علیه امکانات رایانه‌ای، الکترونیکی و سایبریِ رقیب یا دشمن، اقداماتی انجام داد، جنگ و به تبع آن دفاع سایبری معنا یافت(مآبن،[5] ۲۰۱۳: ۶). رسانه‌های اطلاعاتی و ارتباطی نیز، از ابتدای تولّد در راستای اهداف مختلف به کارگیری شدند، خواه این اهداف، سیاسی، فرهنگی،

1. Cyber Mobilization
2. Cyber Terrorism
3. Cyber War
4. Cyber Culture
5. Maa Benn

اجتماعی، اقتصادی یا نظامی و امنیتی باشند(کمیسیون اروپا،[1] ۲۰۱۳: ۴). اهمیت فضای مجازی وعملیات درآن تاحدّی است که ایالات متحدهٔ آمریکا هم اخیراً بودجهٔ اختصاص داده شده به عملیات سایبری را افزایش داده(وبگاه تریپ وایر،[2] ۲۰۱۳) و برای درگیری‌های سایبری و طلوع عصر جدید امنیت ملی، آماده می‌شود(ترایزینگام و کالبرگ[3]، ۲۰۱۳) و عنوان می‌دارد حضور واقدام مؤثر درفضای مجازی، ازمأموریتها و اولویتهای قرن بیست و یکم نیروهای مسلّح ایالات متحدهٔ آمریکا برای پایداری رهبری جهانی این کشور است(اویرنو و مک‌هوگ،[4] ۲۰۱۳). با گسترش حملات و جرایم سایبری، نحوهٔ برخوردباآنها نیز نیاز به توسعهٔ متناسب دارد. در طول سیر صعودی فنّاوری، معمولاً در اکثر کشورها وحتی درشمول جهانی آن، قوانین همواره عقب‌تر از پیشرفت فنّاوری بودندواینترنت نیز مستثنااازاین روند نبوده است. با گسترش شبکهٔ جهانی اطلاع‌رسانی(اینترنت)به دلایلی،جرایمی درمحیط‌های مجازی به وقوع پیوسته که سیستم قضایی کشورهای مختلف نتوانسته‌اند با آنها برخورد جدّی کنند.همین امر باعث شده که شبکهٔ اینترنت، فارغ از سلطهٔ قوانین در دنیا و فضای مستقر خود، به راه خویش ادامه دهد.(حسن‌بیگی، ۱۳۸۴: ۱۴)

فنّاوری اطلاعات، فرصتهای بی‌نظیری رادراختیار بشریت قرار داده، ولی مشابه با هر فنّاوری نوظهور در جهان، چالشهایی نیز به دنبال داشته است. سرقت اطلاعات، خرابکاری، از کاراندازی سیستم‌های رایانه‌ای، کلاهبرداری و جاسوسی، از جمله تأثیرات مخرّب فنّاوری اطلاعات برای حیات بشری است. توسعهٔ اینترنت و گسترش آن حتی به درون منازل و محلهای کارمردم و نیز جهان شمول بودن و وجودخطرات بالقوهٔ آن، سازمانها و دولتها را با چالشهای جدیدی روبه‌رو کرده است(همان: ۱۵). برای نمونه، دولت آمریکا در راهبرد جدید خود، حملهٔ سایبری را معادل حمله به خاک این کشور تلقّی و فرماندهی سایبری آمریکا[5] را برای جنگ ودفاع سایبری ایجاد وسازماندهی کرده است. اهمیت جنگ و دفاع سایبری امروزه به حدّی افزایش یافته که کشورهایی نظیر آمریکا،انگلیس،روسیه،چین،کره،آلمان وحتی رژیم صهیونیستی، به سازماندهی مردمی در خصوص این امر در رسانه‌های مجازی اقدام می‌کنند. جنگ سایبری واقعی، یک رویداد با ویژگی‌های جنگ متعارف است، اما به طور انحصاری طرفین درفضای مجازی می‌جنگند(سومر و براون، ۲۰۱۱: ۲۵). جنگ

1. The European Commission
2. TripWire.com
3. Thuraisingham and Kallberg
4. Odierno and McHugh
5. USCYBERCOM

سایبری امروزدرفضای شبکه‌های اجتماعی سایبری است(ضیائی‌پرور، ۱۳۸۷: ۲۱). میدان جنگ، عرصهٔ سایبر است و سلاحها، تسلیحات سایبری. رشد و گسترش فناوری اطلاعات و اینترنت، آسیبها و تهدیدهایی نظیر جاسوسی صنعتی و اینترنتی را در بر داشته است. فنّاوری، به ویژه ریزپردازنده‌ها، رایانه‌ها و شبکه‌های جهانی، موتور محرّکه‌ای هستند که با سرعتی وصف‌ناپذیر ما را وارد عصر اطلاعات کرده‌اند(بونی و کواسیج، ۱۳۸۳: ۲۹). لذا در برنامه‌ریزی‌های راهبردی سایبری، بایستی نقش، قابلیتها و توان بالای جاسوسی صنعتی و اینترنتی لحاظ شود.

امروزه به طور میانگین هر روز حدود ۱۵۰،۰۰۰ ویروس رایانه‌ای در اینترنت در گردش است و روزانه ۱۴۸،۰۰۰ رایانه به خطر می‌افتد(کمیسیون اروپا، ۲۰۱۳: ۵) واز آنجا که اکثر متخصصان، دانشجویان، دانش‌آموزان و اساتید دانشگاهها در امور روزمره، از فنّاوری‌های دیجیتال، شبکه‌ها و خدمات اینترنت استفاده می‌کنند و تعداد زیادی از شهروندان از طریق اینترنت خرید و فروش می‌کنند و حتی در برخی کشورها و اتحادیهٔ اروپا، بخش فنّاوری اطلاعات و ارتباطات به تنهایی تقریباً شش درصد تولید ناخالص داخلی را شامل می‌شود؛لذا حوادث متأثر بر امنیت سایبری، کسب و کار وشانس دولتها را برای رشد اقتصادی درمعرض خطرقرار داده است(همان: ۵۶). عدم توجه به امنیت اطلاعاتِ شبکه‌های خدمات عمومی، می‌تواند خدمات حیاتی و عملکرد کسب وکار را مختل کند و منجر به ایجاد خسارات مالی قابل توجهی برای اقتصاد کشورها شده، تأثیری منفی برخدمات و رفاه اجتماعی بگذارد(اتحادیه اروپا،[1] ۲۰۱۳: ۵۷). مهم‌ترین نگرانی دراین باره، تهدید ناشی از حملات سایبری سازمان‌یافته است که قادر به تحمیل لطمه‌های جبران ناپذیر به زیرساختهای حیاتی کشورهاست. قدرمسلّم آن است که همگام باتوسعهٔ روزافزون فضای سایبر، ابزارها و شیوه‌های مختلف تهاجمی نیز به سرعت گسترش یافته و توان تخصصی و درجهٔ پیچیدگی نفوذگرانِ عامل تخریب یاغارت، سیر صعودی پیداکرده است(صالحی امیری و همکاران، ۱۳۸۷: ۱۴۸). اگر امنیت اینترنتی نسبت به راهبرد سایبری ملی، درمسیری متفاوت باشد، بسیار مشکل ساز و باعث ایجاد شکاف و ضعف می‌شودکه می‌تواند توسط گروههای متخاصم مورد سوء استفاده قرار گیرد(ترایزینگام و کالبرگ، ۲۰۱۳: ۱۶). سیستم‌های اطلاعات دیجیتال، به ویژه اینترنت، می‌توانندتوسط اشتباهات بشر، حوادث طبیعی، خرابی‌های فنی یاحملات مخرّب، تحت تأثیر قرارگیرند. اختلال در یک کشور می‌تواند اثر جانبی درسایرکشورهای مرتبط داشته و امور خدمات عمومی مردم را مختل کند(اتحادیه اروپا، ۲۰۱۳: ۵۶). حتی

1. Europa.eu

گاهی با دستکاری سابقهٔ جستجوی قربانی و اطلاعات به دست آمده از این طریق، می‌توان او را با تهدید جدّی مواجه کرد.(لی و روتولونی،[1] ۲۰۱۳: ۱۰)

برای فضای مجازی، همان هنجارها، اصول و ارزشهای حاکم بر دولت، باید به صورت برخط اعمال شود.حقوق اساسی وحاکمیت قانون بایددر فضای مجازی محافظت شود. راهبرد برجستهٔ دولت در فضای مجازی بایستی درراستای کاهش شدید جرایم اینترنتی و جنایات سازمان‌یافته باشد.حوادث امنیتی سایبری درحجم بزرگی درحال افزایش است و رفته رفته پیچیده‌ترمی‌شود.این حوادث می‌توانند صدمهٔ عمده‌ای به امنیت واقتصاد بزنند(کمیسیون اروپا، ۲۰۱۳: ۱۵). استفاده از رایانه و اینترنت،مانند تیغ دولبه‌ای است که چنانچه در اختیار دانش‌پژوهی قرار گیرد، در راه صلاح و سازندگی جوامع واگر در اختیار نااهلان باشد، در جهت تباهی جوامع و انسانها به کار می‌رود.(آیکاو و همکاران، ۱۳۸۳: ۱۵)

دی آنجلیز، دیدگاه روشنی از موارد اساسی ارتباط میان جرم و رایانه را ارائه می‌کند و به ویژه بر نیاز به حفاظت ازمفاهیم باارزشی چون: امنیت و حریم خصوصی که اهمیت بسیارزیادی درجامعه دارند، تأکید و بیان می‌کندکه رایانه‌ها تأثیر ضد و نقیضی در دموکراتیزه کردن جرم داشته‌اند. خطرات بالقوهٔ هرزه‌نگاری و تروریسم سایبری، قابل توجه بوده است. با توجه به خواص فضای سایبر، گروههای جدیدی از مجرمان، به سوی جرایم سایبری کشیده می‌شوند و انواع سنّتی جرایم با واقعیتهای روزانطباق می‌یابند(آنجلیز، ۱۳۸۳:۶). به طور نمونه، جوزف نای[2] عنوان می‌دارد: «طی اعتراضات دانشجویی سال ۲۰۰۹م. در ایران، توییتر و سایتهای شبکه‌های اجتماعی برای سازماندهی و گزارش تظاهرات معترضان، اقدامی حیاتی کردند.دولت آمریکا از مدیران توییتر خواست که سرعت سایتها را به منظور انجام تعمیرات از قبل برنامه‌ریزی شده پایین نیاورند. آنها نگران بودند که این کار ممکن است در نحوهٔ سازماندهی اعتراضات با استفاده از توییتر اخلال ایجادکند. با این حال، شش ماه بعدگروهی ناشناس موسوم به ارتش سایبری ایران باموفقیت توانست ترافیک را به وب‌سایتی حاوی یک پیام ضدآمریکایی هدایت کند و در فوریهٔ ۲۰۱۰ (بهمن ماه ۱۳۸۸) دولت ایران توییتر و سایتهای دیگر را مسدودکرد»(نای، ۱۶:۱۳۹۰). این بیان جوزف نای نشان می‌دهدکه ظاهراً وی برآورد صحیحی از اوضاع داخل ایران درآن مقطع زمانی نداشته است؛ زیرا هر چند اقدام شبکه‌های اجتماعی مجازی نظیر توییتر و فیس‌بوک در آن مقطع، درامنیت داخلی ایران، مؤثر بود، اما تنها عدم انجام تعمیرات مقطعی توسط توییتر، اقدامی حیاتی بر

1. Lee & Rotoloni
2. Joseph Nye

ضد امنیت ملی ایران نبود، بلکه این عامل درکنار عوامل دیگر تأثیری نسبی داشته است.

با اینکه از پیشرفت سایبری، منافع قابل توجهی حاصل شده، ولی درعین حال،آسیب‌پذیری سایبری را هم افزایش داده است(ویلشوسن،[1] ۲۰۱۳: ۲۰۵). درتهاجم ازطریق شبکهٔ اینترنت،حتی کشورهایی که به دلیل موقعیت جغرافیایی از بسیاری از تهاجم های فیزیکی مصونیت دارند نیزدرامان نخواهندبود؛ زیرا درفضای مجازی، مرزهای کشورهامفهوم چندانی ندارد و اطلاعات بی‌محابا از مرزبندی‌های سیاسی، اخلاقی و اجتماعی عبورکرده،تبادل می‌شوند. لذا مهاجمان رایانه‌ای قادرند بدون کوچک‌ترین هشداری به شبکه‌های ملی یورش برده، باچنان سرعتی گسترش یابندکه بسیاری ازمواضع هدف، حتی فرصت شنیدن صدای آژیرخطر را نیز پیدا نکنند و حتی درصورت هشدار قبلی هم به احتمال زیادفرصت لازم را برای محافظت ازخود نداشته باشند. از این جهت لازم است تادرسطح ملی ضمن شناسایی نقاط ضعف و قوت و نیز آسیب‌پذیری‌های احتمالی و با در نظر گرفتن فرصتها، اقدامات بازدارندهٔ متناسب، پیش‌بینی و چاره‌اندیشی شود(صالحی امیری و همکاران، ۱۳۸۷: ۱۴۹). تهدیدهای حملات سایبریِ فراگیر علیه دولتها، می‌توانندبه حدّی جدّی باشندکه منجر به تأثیر بر امنیت ملی، اقتصاد و بهداشت عمومی و سلامت شوند. تعداد حوادث سایبریِ گزارش شده همچنان رو به افزایش است.در نتیجه، سرقت داده‌ها، کلاهبرداری اقتصادی ونقض حریم خصوصی افزایش یافته است(ویلشوسن، ۲۰۱۳: ۲۰۵). در سالهای اخیر، زمینه‌های متوجه امنیت فضای مجازی، تغییرکرده و حملات سایبری، با برنامه‌های ملی متمرکز، کسب و کار و دولتها را مورد هدف قرار داده‌اند که در نشت اطلاعات حساس و حیاتی تأثیر بسزایی داشته است(لی و روتولونی، ۲۰۱۳: ۲۵). اگرچه اکثریت قریب به اتفاق حملات سایبری،که در مورد آنها نگرانی‌هایی ابراز شده، تنهابر روی رایانه‌های متصل به اینترنت روی داده است(سومر و براون، ۲۰۱۱: ۳۳)؛ اما امروزه، حمله به سایر شبکه‌های رایانه‌ای کوچک‌تر، نظیر اینترانت‌ها هم گسترش یافته است.

با توجه به مطالب پیش‌گفته، می‌توان گفت که آفند و حملهٔسایبری، استفاده از امکانات و روشها و منابع سایبری برای تأثیر یا تخریب منابع دشمن یا رقیب است؛ به طوری که باعث تأثیرمنفی درامنیت دشمن و تهدید او یا تأثیر مثبت برامنیت ملی خودی باشد.پس جنگ سایبری؛ اقدام به آفند سایبری ازسوی یک گروه یا دولت علیه یک گروه یا دولت دیگر و متقابلاً اقدام به دفاع و پدافندسایبری از سوی دشمن یا رقیب وی است و پدافندسایبری؛ بهره‌جویی ازمنابع مختلف انسانی، مادی، معنوی، فیزیکی، فنی و سایبری است برای دفاع درمقابل حملات وجنگ

1. Wilshusen

سایبریِ طرف مقابل که این طرف مقابل می‌تواند کشور یا گروه رقیب یا دشمن باشد(بیات، ۱۳۸۸). برنامه‌ریزی دفاع و پدافند[1] برای آمیختن دنیای مجازی،[2] با آسیبها و خسارات و معایب فیزیکی محدود دنیای واقعی[3] همراه است(شیمال و ویلیامز،[4] ۲۰۱۱: ۱۰۰) و پدافند سایبری، دفاع در مقابل آفندسایبری است.

برخی کارشناسان بُعد پنجم قدرت راپس از ابعاد زمینی، دریایی، هوایی و فضایی، در عرصهٔ سایبر و فضای مجازی، تحت عنوان قدرت سایبری می‌شناسند و درحال حاضر، ایران را پنجمین قدرت سایبری جهان معرفی می‌کنند(گرداب، ۱۳۹۲). روزانه ۱۳ تا ۱۴ هزارحملهٔ اینترنتی علیه کشورایران صورت می‌گیردکه تقریباً همهٔ آنها در دروازه‌های ورودی کشور مهارمی‌شود.(خبرآنلاین، ۱۳۹۱)

دربین سالهای۲۰۱۰ تا ۲۰۱۳ یک سری تهدیدهای سایبری علیه ایران اعمال شدند که منشأ صهیونیستی- آمریکایی داشتند؛ از جمله حملهٔ ویروسهای استاکسنت،[5] فلیم،[6] دوکو[7] و... به تأسیسات زیرساختی ایران(گرداب، ۱۳۹۲). این تهدیدها به گونه‌ای بودکه تبلیغاتِ بسیاری ازطریق طرفین درفضای مجازی و رسانه‌ها درخصوص آنها انجام شد. در این نبرد، ایران عنوان داشت که توانسته است حملات این ویروسها و بدافزارها را کنترل کرده، مانع صدمه زدن آنها به تأسیسات حیاتی کشور شود. هر چند دشمنان ایران دراین عرصه بهره‌برداری‌هایی کردند که حداقل سودآن برای طراحان بدافزارها این بودکه مطمئن شدند می‌توانند از این طریق به ایران ضربه بزنند و در عملیات روانی علیه جمهوری اسلامی ایران از این روش استفاده کنندیا حداقل مدتی، ذهن راهبرد شناسان و سیاستمداران و متخصصان آن رامشغول کنند.مطالب عنوان شده گویای آن است که نیاز به دفاع و پدافند سایبری برای جمهوری اسلامی ایران، امری لازم به نظر می‌رسد.

امنیت ملی

امنیت در دو مفهوم فردی و جمعی قابل بحث است. امنیت فردی؛ در موضوع حفظ یا تهدید منافع فردی در مقابل تهدیدهای فرد یا جمع دیگر و امنیت جمعی؛ در موضوع حفظ یاتهدید منافع جمعی بحث می‌کند. از آنجا که زندگی انسان در راستای تأمین منافع، امنیت و سلامت استوار بوده، به قول پیامبر اعظم اسلام(ص)،

1. Defence Planning
2. Virtual World
3. RealWorld
4. Shimeall and Williams
5. Stuxnet
6. Flam
7. Doku

معمولاً امنیت و سلامت از نعمتهای مجهول الهی بوده است(پاینده، ۱۳۸۵: ۶۷). امنیت درزبان عربی به معنای بی‌هراس بودن و آرامش است. دایره‌المعارف بزرگ لاروس ذیل واژۀ امنیت[1] آورده است: وضعیتی که شخص درآن از خطر واهمه ندارد و آرامش نفسانی از آن حاصل می‌شود. در واژه‌نامه دبوهم از امنیت این مفاهیم به دست می‌آید: حالت نفسانی قابل اعتماد و آرام که انسان خود را مصون از خطا می‌یابد و وضعیت و حالت آرامی که ازفقدان خطر به دست می‌آید. در زبان انگلیسی نیز ذیل واژۀ امنیت، حالت یا احساس آزاد بودن از ترس و بیمناکی آمده است. مسئلۀ امنیت، نگرانی کشوری خاص نیست و مربوط به تمام کشورهاست(مورگنتا، ۱۳۸۹: ۶۸۴). برخی معتقدند مفهوم امنیت ملی، ساخته و پرداخته در ایالت متحده و توسعه یافته در جهان غرب است(عبدالله‌خانی، ۱۳۸۹: ۱۴۱). واژه امنیت ملی مانند دیگر مفاهیم علوم انسانی، دارای مفاهیم متعدد و پیچیده است که ریشۀ آن درتلقی و برداشت متفاوت افراد، گروهها و کشورها از این مفهوم است. برهمین اساس، آرنولدولفرز می‌گوید: امنیت ملی نماد ابهام‌آمیزی است که اصلاً ممکن نیست دارای معنای دقیق باشد. بوزان هم می‌گوید: سیاستمداران از اینکه مفهوم امنیت را مبهم و نامشخص نگه دارند، کاملاً خوشحالند؛ زیرا در حمایت از اهداف متنوع، بهتر می‌توان بدان تمسّک کرد.(بشیری، ۱۳۸۸: ۱)

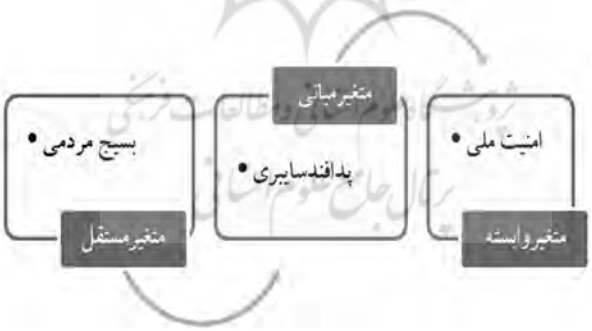
درطول تاریخ حیات بشر، زمانی امنیت صرفاً در موضوع تهدیدها و بلایای طبیعی مانند سیل، زلزله، آتشفشان، صاعقه یا حیوانات درنده و نظایر آن قرار داشت. اما به تدریج جای خود را به ترسِ انسان از انسان یا گروه انسانها از انسانها داد و امروزه با گذر از دوران سنّتی، کلاسیک و مدرن و ورود به عصر فرامدرن، بحث امنیت جهانی و حرکت به سوی همگرایی و همکاری‌های منطقه‌ای و جهانی مطرح شده است. امنیت، اصطلاحی است که بر نبود تهدید نسبت به ارزشهای اساسی یک ملت دلالت دارد. ازنظرتاریخی،امنیت به عنوان ارزش پایه‌ای و هدف نهایی رفتار دولت تلقی شده است. امنیت؛ یعنی نبود تهدید و تهدید، هر عنصر یا و ضعیتی است که موجودیت و ارزشهای حیاتی را به خطر بیندازد(دانشگاه امام حسین، ۱۳۷۶: ۵). بهشت کامل انسانی جایی است که انسان درآن از همه نوع امنیت و آرامش برخوردار باشد. اگر دغدغۀ آرامشِ روحی و روانی برای هر فردی، دغدغه و هدف اصلی است، آرامش و امنیت جمعی نمی‌تواند از این دایره بیرون باشد. لذا امنیت و آرامش به شکل لایه‌های درهم تنیده خودنمایی می‌کند. بنابراین، تلاش انسان برای دستیابی به همۀ انواع و اقسام آرامش و امنیت و حفظ و نگهداشت آن است.(توکلی،۱۳۸۹)

1. Security

برخی، شاخصه‌های سرزمین، حکومت و جمعیت را سه مؤلفهٔ امنیت ملی می‌دانند. درسالهای اخیر نظریه‌پردازان بر این باورند که پنج مؤلفه درمبحث امنیت ملی نقش تعیین‌کننده دارندکه عبارتند از: نیروهای مسلّح، مقبولیت و مشروعیت عام، اقتصاد و توانمندی مالی حکومت، دسترسی به منابع حیاتی وحساس و مدارای قومی مذهبی(تبیان نیوز،۱۳۹۱). می‌توان گفت امنیت ملی؛ یعنی دستیابی به شرایطی که به یک کشور امکان می‌دهد ازتهدیدهای بالقوّه یا بالفعل خارجی و نفوذ سیاسی و اقتصادی بیگانه در امان باشد و در راه پیشبرد امر توسعهٔ اقتصادی، اجتماعی و انسانی و تأمین وحدت و موجودیت کشور و رفاه عامه، فارغ از مداخلهٔ بیگانه گام بردارد(بشیری، ۱۳۸۸: ۱).دراثر پیشرفت وتوسعهٔ فنّاوری اطلاعات،امنیت ملی و اقتصادی کشورها وابستگی روز افزونی به فنّاوری اطلاعات و زیرساختهای اطلاعاتی پیداکرده و فنّاوری‌های دفاع و امنیت در برابر تهدیدکنندگان فضای سایبر باسرعت کمتری درحال توسعه است؛ یعنی بین گسترهٔ کاربردهای فنّاوری اطلاعات و فنّاوری‌های دفاعی و امنیتی آن، فاصله و «شکاف آسیب‌پذیری» افتاده است که به عنوان یک معضل جدّی برای کشورها، روز به روزدر حال افزایش است.(صالحی امیری و همکاران، ۱۳۸۷)

الگوی مفهومی موضوع

با توجه به توضیحات ارائه‌شده،متغیّرهای موضوع این مقاله عبارتند از: ۱. بسیج مردمی؛ ۲. پدافند سایبری؛ ۳. امنیت ملی ج.ا. ایران.



شکل۱-ارتباط مفهومی متغیرهای موضوع مقاله

مفهوم «امنیت ملی» و «دفاع» با همدیگر و با مفهوم «قدرت» ارتباط تنگاتنگ دارند.زمانی دفاع تجلّی عینی داردکه امنیت آدمی مورد هجوم واقع شود. دفاع یعنی دفع تجاوز درحوزهٔ امنیتی زندگی درابعاد فردی و اجتماعی انسانی. امنیت ملی درسایهٔ قدرت ملی حاصل می‌شودودفاع دربرابر مهاجم، مستلزم وجود «قدرت» است(مطهرنیا، ۱۳۷۶: ۳۷). باتوسعه فنّاوری اطلاعات و ارتباطات و فضای سایبری،

تهدیدهای سایبری نیز گسترش یافته، لزوم اتخاذ تدابیر دفاعی و پدافندی سایبری احساس می‌شود. براین اساس، باتوجه به ابعاد و مؤلفه‌های قدرت ملی و امنیت ملی، سه متغیّر بسیج مردمی، پدافند سایبری و امنیت ملی در ارتباطی تنگاتنگ با همدیگرند. به نظر می‌رسد با بسیج مردمی می‌توان سطح دفاع سایبری را ارتقا داد و منجربه افزایش ضریب امنیت ملی شد.

تعاریف مفاهیم اساسی موضوع

بسیج مردمی؛ عبارت است از جهت‌دهی و بهره‌برداری از حرکاتِ خودجوشِ افراد و گروهها یا استفاده از توان نیروهای مردم به طور سازماندهی شده، در راستای رسیدن به اهداف یک گروه، سازمان یا دولت و به طور خاص اهداف امنیت ملی در یک کشور.(بیات، ۱۳۹۲: ۶)

پدافند سایبری؛ یعنی هر اقدام و استفاده از امکانات، روشها و منابع مختلف انسانی، مادی، معنوی، فیزیکی، فنی و فضای مجازی، برای دفاع، پیشگیری و مقابله با تهدیدها و اثرات آفند و حملات فضای مجازی توسط طرف مقابل(کشوریا گروه رقیب یا دشمن). پدافندسایبری، دفاع در مقابل آفندسایبری است. هر چند برخی با لحاظ نظرات فنی، بین تعریفِ پدافند سایبری ودفاع سایبری تمایز قایلند، اما در این مقاله، با لحاظ منظور کلی و عام به این دو، تعریفی یکسان در نظر گرفته شده است.(همان: ۶)

امنیت ملی[1]؛ عبارت است از توانایی یک کشوردر دفع تهدیدهای خارجی علیه حیات سیاسی یا منافع ملی خود. به عبارت دیگر؛ امنیت ملی یعنی دستیابی به شرایطی که به یک کشور امکان می‌دهد از تهدیدهای بالقوّه یا بالفعل خارجی و نفوذ سیاسی و اقتصادی بیگانه در امان باشد و در راه پیشبرد امر توسعهٔ اقتصادی، اجتماعی و انسانی و تأمین وحدت و موجودیت کشور و رفاه عمومی، فارغ از مداخلهٔ بیگانه گام بردارد.(بشیری، ۱۳۸۸: ۱۵۲)

اینترنت و فضای مجازی

رسانه‌های اطلاعاتی و ارتباطی وقتی به اوج اثر خود می‌رسندکه از حالت تک‌مخاطبی، خارج و به صورت شبکه‌ای مورد استفاده قرارگیرند. فکر ایجاد شبکه دردههٔ ۶۰ میلادی و با این مضمون به وجود آمدکه چگونه می‌توانیم پیامهای اطلاعاتی را روی یک رسانهٔ ارتباطی به صورتی کارا و قابل اعتماد ارسال کنیم؟ پس از آن، با

1. National Security

تحولاتی که دراین زمینه به وجود آمد، از اواسط دهۀ ۷۰ تلاش شد تا سرویسهای ارتباطی را روی یک مجموعه از شبکه‌های به هم متصل تدارک ببینند. به این ترتیب، سنگ بنای تبادل وسیع و هماهنگ «داده» که امروزه یکی از بخشهای مهم کار با رایانه است، گذاشته شد.این فنّاوری جدید، «ارتباط بین‌شبکه‌ای»[1] یا اینترنت نام دارد(حسن‌بیگی، ۱۳۸۴: ۱۹) که از مهم‌ترین رسانه‌های ارتباطی و اطلاعاتی است که گام بزرگی درحوزۀ فاوا[2] به شمار می‌رود. اینترنت، مجموعه‌ای از شبکه‌های رایانه‌ای به هم پیوسته در کل جهان است که آن را می‌توان از طرق مختلف به مثابۀ نقشۀ شاهراه ارتباطاتی دانست.(بونی و کواسیچ، ۱۳۸۳: ۵۸)

به دنبالِ استفادۀ گستردۀ کاربران؛ دانشگاهها، مراکزدولتی و شرکتهای معتبر خود را به اینترنت متصل کردند و شبکه‌های اطلاعاتی گسترده‌ای را روی اینترنت قرار دادند(مرادی، ۱۳۸۹: ۴۶). در امور تجاری، اینترنت به مثابه مقابلۀ داود با جالوت است؛ یعنی منافع و مزایای اینترنت به قدری است که با وجود خسارات احتمالی، نمی‌توان آن را نادیده گرفت(بونی و کواسیچ،۱۳۸۳: ۶۱). امروزه، اینترنتِ قابل اعتماد و دیگر امکانات رایانه‌ای مطمئن، از ضروریات زندگی است(سومر و براون، ۲۰۱۱: ۱۶). از مهم‌ترین شاخصه‌های اینترنت، «تعامل» است. تعامل اینترنت پایه[3] یا تعامل بر مبنای شبکه اینترنت، می‌تواند گروهها و افراد سازمانهای بسیاری را در یک شبکۀ چند وجهی با یکدیگر مرتبط کند تا با به وجودآوردن این تعامل، در مسیر به وجودآوردن تفاهم و از میان برداشتن مرزهای فیزیکی و تا حد امکان مرزهای ذهنی گام بردارند(کلهر، ۱۳۸۶:۱۵). اینترنت گسترۀ وسیعی است که سیاست و منازعات سیاسی ازنوع سایبری آن را، تحت تأثیرخود قرارداده(کارازوجیانی، ۱۳۸۸: ۳۳)، چالشهای جدیدی فرا روی کارشناسان امنیتی و مجریان قانون گذاشته است(بونی و کواسیچ، ۱۳۸۳: ۶۰). از دید برخی دیگر، اینترنت اساساً واقعیتی است که باعث ارتباط واتصال میلیونها رایانه درسراسرجهان شده است. اینترنت، ساختاری است برای برقراری روابط میان اندیشه‌ها، روشها و پردازشهای دیجیتالی و ابزاری است بدیع و منسجم با فنّاوری پیشرفته و مدرن اطلاعاتی وتعداد نامحدودی کاربر در فضای مجازی مشترکی که مرزهای جغرافیایی ملی و منطقه‌ای، آن فضا را محدود نمی‌کنند.(مرادی، ۱۳۸۹: ۴۹)

اصطلاح فضای سایبر برای اولین بار در سال۱۹۸۲م. دریک داستان علمی-تخیّلی به کار برده شد. فضای سایبر، محیطِ ارتباطیِ فرستندۀ یک پیام باگیرندۀ آن است.

1. Internet Working / Internet

۲. فنّاوری اطلاعات و ارتباطات.

3. Internet-Based Interaction

با این تعریف، فضای سایبر اگر چه اصطلاحی به نسبت جدیداست، اما مفهوم آن جدید نیست و پیدایش این مفهوم، همزمان با اختراع تلفن توسط الکساندر گراهامبل درسال ۱۸۷۶م. بوده است(آنجلیز،۱۱:۱۳۸۳). فضای مجازی؛[1] یعنی محیط تبادل اطلاعات و ارتباطات بین انسانها در بستر فنّاوری‌های رایانه‌ای و مخابراتی(بیات، ۱۳۹۱). فضای سایبر استعاره‌ای برای تشریح سرزمین غیر فیزیکی تشکیل شده توسط سیستم‌های رایانه‌ای است. درفضای سایبر نمی‌توان بویید یا شنید(منظور توسط حواس رایج است).(سیدمفیدی،۱۸:۱۳۸۳)

برخی نظیر رابینز و وبستر، ارتباط فضای سایبر با فضای حقیقی و واقعیتهای جهان راگسسته دانسته، عنوان می‌کنند: «فضای سایبرنتیکی، فضایی منزوی است؛ یعنی چیزی که تماس خود با واقعیتهای جهان را ازدست داده است و در نتیجه، در هماهنگی با این اعتقاد عمل می‌کند؛جهانی که اکثر ما هنوز در آن می‌خواهیم زندگی کنیم دیگر هیچ واقعیتی ندارد»(رابینز و وبستر،۲۶۸:۱۳۸۴). البته با اندکی تأمل می‌توان این گفتهٔ وبستر و رابینز را رد کرد و نه تنها می‌توان گفت که فضای سایبرنتیکی، فضایی منزوی نیست و تماس خود با واقعیتهای جهان را از دست نداده، بلکه نوعی شبیه‌سازی از آن و نوعی واقعیت مجازی[2]است.

شبکه‌های اجتماعی مردمی در فضای مجازی

فضای سایبر امروزه یکی ازمهم‌ترین وپرکاربردترین رسانه‌های اجتماعی به نام شبکه‌های مجازی اجتماعی رادراختیارکاربران قرارداده است. رسانه‌های اجتماعی ابزاری برای تأثیرگزاری برافکارعمومی جامعه به شمار می‌روند(کارازوجیانی، ۱۳۸۸: ۲۰). شبکه‌های مجازی، از این جهت که همهٔ آنها رسانه‌اند، خصلتهای رسانه بودن رادارند؛ اما ماهیت آنها متفاوت است.آنها دارای ماهیت جدیدی‌اند که مربوط به لافضا و لامکان بودن آنهاست(مرکزتوزیع پیام دیدار،۱۳۹۱: ۸). در جوامع شبکه‌ای، چهارعنصر اساسیِ همبستگی، انتشار، بسیج و مشاهده و بررسی، در شکل دادن به یک حرکت جدّی، مؤثرند و می‌توانند بسیاری از نهادها وافراددرون جامعه را به سمت شبکه‌ای شدن و حرکت توده‌وار و با عزم روشن و هدف متعالی؛ یعنی ارتباطات، بسیج را منسجم کنند(کلهر، ۱۳۸۶: ۸). یکی از ابزارهای اساسی برای مقابله با تهاجم گستردهٔ فرهنگی دشمن و جنگ درحوزهٔ نبرد نرم وفرهنگی، استفاده ازفضای مجازی و راه اندازی بسیج شبکه‌ای بااستفاده از پتانسیل اینترنت است. این حوزه که با هزینهٔ به نسبت

1. Cyber Space
2. Virtual Reality

کم، با جمع‌آوری توان محدود افراد متفرقه‌ای که با هویت دینی وانقلابی دراقصا نقاط عالم به فکرحفظ و اعتلای فرهنگ دینی می‌باشند، می‌تواند قدرت عظیمی از لحاظ فکری به افراد اعطا کند؛ با افزایش ضریب نفوذ محتوایی مطالب دینی به زبانهای مختلف، اقدام به مقابله باتهاجم فرهنگی و هویتی غرب کرده و حتی با به نقد کشیدن اساسِ باورهای غرب، مبانی معرفتی آنها را با چالش جدّی مواجه کرده است(مرادی،۱۳۸۹: ۱۳۰). درعصر سایبر، جهان جدید به شبکهٔ نیرومندی تبدیل شده است که بافت اصلی و تاروپود آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در درون این شبکه، به جز گروهی از نخبگان، دیگران کنترل خود را برزندگی خویش و محیط پیرامون از دست داده یا به سرعت درحال ازدست دادن آنند.(عباسی وهاشمی، ۱۳۸۹: ۵۶)

با گسترش اینترنت و به خصوص با تولد وب دو،[1] شبکه‌های مجازی توسعه یافتند و به راحتی گروهها و انجمنهای اینترنتی، با سیستم‌های کاملاً هوشمند نرم‌افزاری و سخت‌افزاری گره خوردند و در راستای آمال بشری به کارگرفته شدند. چنانچه امروزه شاهدیم، دست اول‌ترین اخبار و تحلیلها و پرونده‌های صوتی و تصویری از وقایع مختلف جهان درشبکه‌های مجازی نظیرفیس‌بوک، توییتر[2] و... در سریع‌ترین زمان درج و پخش می‌شوند. به طور نمونه، اخبار و تصاویر مراسم تودیع پروفسور ثبوتی[3] در زنجان که با حاشیه‌هایی روبه‌رو بوده، حتی قبل ازجمع‌آوری توسط مأموران امنیتی و رسمی دولت، از وب‌سایتهای انگلیسی پخش شد، آن هم گزینشی و در راستای اهدافِ ضدایرانی! نمونه‌های دیگری از چنین اقداماتی گویای آن است که فضای سایبر، عرصه‌ای است که غفلت ازآن درامر بهره‌جویی ازابزاررسانه‌ای و اطلاع‌رسانی،در راستای آسیبها وتهدیدهای امنیت ملی، موجب زیان و پشیمانی خواهد بود(بیات، ۱۳۹۱).همچنین در اغتشاشات وفتنهٔ سال ۸۸ ایران، ابزار رسانه و فضای مجازی درساماندهی آن، بسیارسهیم بوده است.

با عضو شدن گروههای مجازی علمی و تخصصی در اینترنت، آنها می‌توانند در جریان آخرین اطلاعات موجود دررشته‌های تخصصی خود قرار گیرند؛ زیرا همهٔ اعضا درجریان پیامهای علمی که توسط یک نفرصادر می‌شود قرار دارند. آنان می‌توانند اطلاعات تولیدی خود را دراختیار تمامی افرادی که امکان دسترسی به این شبکه را دارند قرار دهند و از آنان نیز بخواهند علاوه بر نظرخواهی، برایشان مدارک علمی مشابهی از همین رهگذر ارسال کنند، یا با خودِ آنان همکاری

1. Web2
2. Twitter
۳. رئیس مرکزتحصیلات تکمیلی علوم پایه زنجان در سال ۱۳۹۰ پس از دو دهه، از ریاست تودیع شد.

مستمر داشته باشند. از آنجا که زمینهٔ هرگونه نوآوری و خلاقیت در پژوهشِ علمی تبلور می‌یابد، پیشرفت فنّاوری‌های جدید و خلاقیتها از دستاوردهای جامعهٔ اطلاعاتی محسوب می‌شود(مرادی، ۱۳۸۹: ۱۱۷). گفته می‌شود ابداعات و اکتشافاتی که در ۵۰ سال گذشته رخ داده، بیش ازکل ابداعات بشری از ابتدای خلقت بشر بوده است(بونی و کواسیچ، ۱۳۸۳: ۴۴). دولتها، نیاز به آمادگی کامل برای مقاومت دربرابر طیف گسترده‌ای از وقایع اینترنتی دارندکه می‌تواند شامل وقایع ناخواسته، تصادفی و عمدی باشد(سومر و براون، ۲۰۱۱: ۵۴). برخی محققان ارتباطات معتقدندکه موفقیت اجتماعات مجازی عملاً به مثابهٔ نشانهٔ زوال اجتماعات واقعی است. انسانهای جوامع مجازی،احساسات و افکارشان را آزادانه بیان می‌کنند و وحدت ویکپارچگی خود را با اجتماعات واقعی از دست می‌دهندو با افراد اجتماعات مجازی همبسته می‌شوند.(مرادی،۱۳۸۹: ۱۲۴)

رابینز و وبستر به نقل از سیواناندان[1] می‌گویند: «اجتماع مجازی، اجتماع علایق است نه اجتماع افراد»(رابینز و وبستر، ۱۳۸۴: ۳۲۹)؛در حالی که امروزه، شبکه‌های اجتماعی مجازی، نه تنها اجتماعی از علایقند، بلکه اجتماعهایی مجازی از افراد نیز هستند. فضای سایبر فراهم کنندهٔ رابطه‌ای است که در آن مردم بی‌نیاز از اتّکا به روابط چهره به چهره می‌توانند دست به تعامل و هماهنگی اقداماتشان بزنند. گروههای مخالف سیاسی می‌توانند صدای رسا داشته باشند بدون اینکه حکومتها به راحتی قادر به ساکت کردنشان باشند. همانند تلاشهای سندر لومینوسو[2]، رهبر چریکهای راه درخشان وحکومت پرو.

اورارد[3] معتقد است که، تدارک انتخابات دراندونزی و سقوط رژیم سوهارتو[4]، تجربه‌ای بود که اینترنت را به بازیگرکلیدی و یکی از مهم‌ترین منابع اطلاعاتی جایگزین تبدیل کرد؛ این درحالی بودکه مقامات، کنترل شدیدی را بر رسانه‌ها اعمال می‌کردند. شاخهٔ چپ حزب دموکراتیک خلق پس از یک سری نا آرامی‌های جاکارتا در جولای ۱۹۹۶، تحت فشار انتقادها و سرزنشهای حکومتی، تبدیل به نیروی زیرزمینی شدند. اما در مقام دفاع از خود، سعی کردند با استفاده از فضای اینترنت، انتقادها و اتهامات علیه خود را پاسخ بدهند(کارازوجیانی، ۱۳۸۸: ۶-۵). نمونهٔ این استفادهٔ همگانی ازفضای مجازی برای مقابله با تهدیدهای دشمن، روش بمب گوگلی درجریان تحریف نام خلیج فارس توسط نشریهٔ کانادایی نشنال جئوگرافیک

1.Sivanandan
2. Sender luminoso
3. Euerard
4. Soeharto

بود که منجر به عقب‌نشینی وعذرخواهی این نشریه شد. همچنین در جنگ۲۲روزۀ غزه، با راه‌اندازی جهاد مجازی برای مقابله با آتش‌افروزی‌های رژیم صهیونیستی، امکان بسیج افکار عمومی در سطح بین‌الملل و حتی در درون کشوررژیم اشغالگر قدس علیه سران آن کشور فراهم شد(مرادی،۱۳۸۹: ۱۲۸). تأثیر شبکه‌های اینترنتی، از نظر سیاستمداران هم دور نمانده است، الگور، معاون سابق رئیس جمهور آمریکا گفته بود: «ما در شُرِف یک انقلاب هستیم که مثل انقلاب صنعتی، تأثیر زیادی بر اقتصاد خواهد داشت. به زودی شبکه‌های الکترونیکی این امکان را برای مردم فراهم می‌کند که مرزها و فاصله‌های زمانی را بشکنند و از فواید بازارها و فرصتهای تجاری جهانی استفاده کنند که امروز حتی تصور ناپذیر است و دنیای جدیدی از امکانات و پیشرفت اقتصادی باز خواهدشد».(بونی و کواسیچ، ۱۳۸۳: ۳۸)

استفاده از فضای مجازی تنها به امر تبلیغ و اطلاع‌رسانی محدود نمی‌شود، بلکه برای آسیب زدن به منافع دشمن و حریف نیز عملیات دارد؛ نظیر حملۀ ویروس لاوباگ[1] که طی آن افزون بر ۵۰ میلیون رایانه مورد حمله قرار گرفتند و حدود چهار درصد از آنها به تعمیر سخت‌افزاری و فیزیکی نیاز پیدا کردند. این حجم از رایانه‌های آسیب‌دیده، باعث شدند سیستم پست الکترونیک بسیاری ازشرکتهای بزرگ و سازمانهای دولتی از قبیل ناسا[2] و مؤسسه‌های آموزشی از کار بیفتد. در برخی از موارد، مدت زمان از کار افتادگی سیستم به ۴۸ ساعت و حتی به یک هفته نیز رسید. تصمیم به خاموش کردن سیستم‌ها اقدامی محتاطانه و مقتضی بود؛ زیرا اگر سیستم‌ها خاموش نمی‌شدند، آسیب وارده بسیار جدّی‌تر می‌شد (آربسکلاو،۱۳۸۷: ۵۴). با ایجاد اینترنت و شبکه‌های رایانه‌ای و فنّاوری اطلاعات و ارتباطات، ابزار مورد استفاده در بحرانها و شورشها و جنگها نیز به مرحلۀ تازه‌ای قدم گذاشتند؛ چون ارسال اخبار و اطلاعات بسیار سریع‌تر از قبل صورت می‌گرفت، حجم انبوه اطلاعات در زمانی بسیار کم از اقصی نقاط جهان به نقاط دیگر آن قابل ارسال شد. انواع ارتباطات چندرسانه‌ای شامل متن، فیلم، صوت و تصویر و... به راحتی در دسترس و قابل نقل و انتقال شد.(بیات، ۱۳۹۱)

بسیج سایبری

فضای مجازی، توانایی بسیج مردمی را به صورت بسیج سایبری به شدت افزایش داده است. گروهها و افرادی که دارای ایده‌ها وآرمانهای مشترکند وبه یکدیگر نزدیکترند، ضمن تعامل با یکدیگر، افزون بر مستحکم‌تر کردن پیوندهایشان، لینک‌های جدیدی را به وجودآورده و گروهها و افراد جدیدتری را نیز به شمار خود

1. Love Bug
2. NASA

می‌افزایند(کلهر، ۱۳۸۶:۱۵). با استفاده از ظرفیتهای بسیج سایبری می‌توان در طراحی عملیات و اقدامات جنگ روانی، کارهای مؤثری انجام داد. در این راستا بایستی مواظب راهبرد ضد بسیج سایبری نیز باشیم (توماس،[1] ۲۰۱۳: ۲۶). اجتماعات مجازی،[2] انواع جدیدی ازاجتماعات راعرضه می‌کنندکه نزدکاربران اینترنت ورسانه‌های مرتبط باآن وآنهایی که به این وسایل جدیدارتباطی واطلاعاتی دسترسی دارند، به نوعی دوگانگی ایجاد می‌کند؛ چرا که رسانه‌های مذکورنوعی مناسبات جدیدایجاد می‌کنندکه دراین مناسبات، انسانها بیش ازپیش گوشه‌گیر،منزوی وکم‌تحرک شده،کم‌کم اززمینهٔ عملی زندگی خود دور می‌شوند. (مرادی، ۱۳۸۹: ۱۲۶)

یکی از وسیع‌ترین کاربردهای مورد بحث فنّاوری‌های شبکه‌ای شده، بسیج برخط(آن‌لاین) است. بسیاری از گروههای معترض اجتماعی بر به وجود آوردن شبکه‌ای از افراد وگروههایی که می‌توان از طریق ایمیل آنها را به یکدیگر مرتبط ساخت، حرکتهای اعتراضی وسیعی چون اعتراضات سیاتل را شکل می‌دهند(کلهر، ۱۳۸۶: ۱۵). ما در حال ورود به دوران بسیج اینترنتی هستیم. اما مسیر فعلی ما تنها امکان واکنش به آثار آن را به ما می‌دهد(کرونین، ۱۳۸۵: ۷۴). وقتی از «بسیج اینترنتی روی شبکه» سخن می‌گوییم، نخست از تلاشهای شبکه‌ای بحث می‌کنیم که مردم را به سمت اقدام، اعتراض، مداخله، حمایت و پشتیبانی حرکت می‌دهد. چنین تلاشهایی بیشتر در مورد ارتباطات و اجتماع است تا اطلاعات(کلهر، ۱۳۸۶: ۱۵). حکومت می‌تواند ابزارهای بسیج مردمی را اصلاح کند و در اختیار بگیرد، اما تنها در صورتی که به نیازهایی چون: درک آنها، واکنش به آنها و به کارگیری آنها جدّی‌تر توجه کند.(کرونین، ۱۳۸۵: ۸۵)

بسیج مردمی شکل‌یافته در گروهها و سازمانهای اجتماعی، امروزه تا اندازهٔ زیادی بر فنّاوری اطلاعات و تجلّی آن؛ یعنی اینترنت مبتنی شده است. بسیج مردمی و حداقل بسیج گروههای مردمی فعال روی اینترنت، وجهی فراملّی یافته و می‌تواند به خوبی مورد بهره‌برداری سازمانها و گروهها قرار گیرد که با ایدهٔ مشترک در بحث یادگیری‌های اینترنتی و ایجاد حرکتهای فراملی علیه یک دشمن مشترکند. حرکتهایی مانند حفظ محیط زیست یا ضدیت با جنگ و... نیز به عنوان اهداف وآرمانهای بالا، موجب بسیج گروهها و افراد و حتی مللی شده که بستر فعالیت آنها تنها اینترنت است. از این رو، گاه به بسیاری از این حرکتها، حرکتهای اینترنت پایه[3] یا برمبنای اینترنت گفته می‌شود. بسیج با توجه به تمرکز بر آرمانهای مشخص و ارزشهای تعریف شده از اینترنت، برای فراگیر کردن این

1. Thomas
2. Vitual Communities
3. Internet-Based Movements

آرمانها بهره‌برداری می‌کند. بسیج امری است که از اندیشه و دل آغازمی‌شود و با ابزاری که بر اندیشه‌هاتأثیربخش است، سروکار مستقیمی پیدا می‌کند و اینترنت در این زمینه سازوکارهایی بسیار فراگیر و اثربخش دارد. غربیان نیز با بهره‌گیری از این فنّاوری بر آن شدند که به نحوی بر قلبها و اندیشه‌هاتأثیرگذار باشند و از رهگذر آن بتوانند برای تفکر انسان در ارائهٔ خرد جایگاه اصیل و وسیعی بیابند.(کلهر، ۱۳۸۶: ۱۷-۹)

شاخصه‌های بسیج مردمی، پدافند سایبری و امنیت ملی

شاخصه‌ها، نمایشگرهای یک متغیّر در عالم بیرون و عالم واقع‌اند. با توجه به بررسی آثار، مصاحبه‌ها و نظر کارشناسان امر، گردآوری میدانی و مشاهده‌ها و تجربیات محقق، برای متغیّرهای مقالهٔ حاضر شاخصه‌های ذیل بیان می‌شوند:

الف) شاخصه‌های بسیج مردمی

۱. وجود مراکز تربیت و آموزش نیروی انسانی ماهر به منظور دفاع در حوزهٔ سایبر؛
۲. وجود و حضور سازمانهایی برای سازماندهی و به کارگیری افراد وفادار به نظام درحوزهٔ دفاع سایبر؛
۳. وجود و حضور افراد داوطلب توانمند و وفادار به نظام در راستای پدافند سایبری؛
۴. حضور اعضای بسیج اقشار در پروژه‌های مربوط به پدافند و دفاع سایبری (بسیج دانشجویی، دانش‌آموزی، اساتید، جامعهٔ زنان، مهندسان و...)؛
۵. وجود شبکهٔ ارتباطی فعالان سایبری همسو با نظام(شامل افراد و نیروهای وفادار به نظام و عوامل و منابع سایبری) نظیر شبکه‌های اجتماعی مجازی و وب‌سایتها و پایگاههای ارتباطی میان اعضای بسیج مستضعفین برای انتقال برنامه‌ها، راهبردها وروشها به اعضا به صورت سریع، دقیق، مناسب و دریافت و تجزیه و تحلیل بازخورد اقدامات این شبکه؛
۶. وجود قوانین مصوّب و حمایت قضایی مناسب برای حمایت از اقدامات فعالان همسو(افراد، عوامل و منابع فضای مجازی) در راستای پدافند سایبری(برای مثال، اگر در مورد خاصی فعالیت هکری با هماهنگی یک سازمان اقدامی صورت گرفته، از نظر سازمان دیگر مجرم شناخته نشود)؛
۷. وجود و حضور سازمانهای مردم نهاد طرفدار نظام که در فضای سایبر فعالیت دارند؛
۸. وجود و انجام پروژه‌های تعریف و عملیاتی شده توسط مراکز علمی و

نهادهای انقلابی طرفدار نظام در راستای پدافند سایبری (جهاد دانشگاهی، دانشگاهها و...)؛

۹. میزان حضور، آمادگی و فعالیت برخط و بهنگام و میزان دسترسی در مواقع لزوم به شبکهٔ بسیج سایبری (افراد، فعالان، عوامل ومنابع سایبری همسو) درراستای اجرای عملیات و اقدامات پدافند سایبری؛

۱۰. میزان پشتیبانی فنی،تجهیزاتی و مالی و معنوی از فعالان و اعضای شبکه عوامل و منابع سایبری.

ب) شاخصه‌های پدافندسایبری

۱. میزان وجود و تولید فنّاوری‌های بومی و ملّی در حوزهٔ سایبر(ضد بدافزار بومی، شبکهٔ ملی دیتا، شبکهٔملی آموزش، مرکز داده‌های بومی، موتور جستجوی بومی، خدمات رایان‌نامهٔ بومی، سیستم عامل های بومی، الگوریتم‌های بومیِ امنیت اطلاعات، هوش مصنوعی، نرم افزار، سخت‌افزار و...)؛

۲. میزان دسترسی شبکهٔ عوامل و منابع و فعالان همسو به وبگاههای همسو؛

۳. کاهش ضریب بهره‌برداری از سایتهای فیلتر شده و غیر مجاز و وبگاههای غیر همسو؛

۴. تعداد پروژه‌های سازمانهای دولتی در پدافند سایبری؛

۵. میزان دانشجویان وفادار به نظام و بسیجی در رشته‌های سایبری(رایانه، فنّاوری اطلاعات و ارتباطات) و متخصصان امر هک و امنیت شبکه نسبت به سایر دانشجویان این رشته‌ها؛

۶. تعداد عملیاتهای سایبری و تعداد وبگاههای هک شده در دهه‌های گذشته(نظیر هک کردن سایتهای حریف و پیشگیری از هک سایتهای خودی، کمپین محافظان قرآن و...) در جهت مقابله و پیشگیری از اقدامات سایبری دشمن؛

۷. وجود هماهنگی و تعامل میان سازمانهای مرتبط با پدافند سایبری(سپاه، بسیج، ناجا، واجا، ودجا، آجا، پدافند غیر عامل و...)؛

۸. وجود زیرساختهای امن و مطمئن سایبری(فیبر نوری و...) و مدیریتِ مؤثرِ کمّیت و کیفیت ارتباطات (افزایش یا کاهشِ قیمت و سرعت اینترنت، پهنای باند و...) در راستای پیشگیری و مقابله با تهدیدهای سایبری دشمن؛

۹. میزان کنترل دسترسی به اینترنت در شرایط غیر عادی و بحرانی برای مقابله با تهدیدهای سایبری دشمن؛

۱۰. وجود مراکز اطلاع‌رسانی در راستای آگاه‌سازی مردم برای پدافند سایبری.

ج) شاخصه‌های امنیت ملّی

با توجه به تعاریف امنیت در دو بُعد سلبی و ایجابی،شاخصه‌های امنیت ملی نیز در دو بخش بیان می‌شوند: نخست اینکه، جلوی تهدیدها را گرفته باشیم و بعد اینکه، امنیت سیستم‌های خود را بالا ببریم.

۱. ارتقای امنیتِ سامانه‌های اساسی ملی و سامانه‌های فنّاوری اطلاعات و ارتباطات؛
۲. ارتقای امنیت بانکهای اطلاعاتی ملی و مراکز داده‌های امن؛
۳. ارتقای امنیت و حفاظت فیزیکی از زیرساختهای سایبری؛
۴. ارتقای سطح مقبولیت و مشروعیت نظام با استفاده از ظرفیت فضای مجازی؛
۵. ارتقای صحّت و سلامت و اعتماد در مدیریت اقتصاد ملی و بازار بورس و تجارت الکترونیک در فضای مجازی؛
۶. ارتقای میزان اشرافیت بر فضای مجازی و رصد فعالیتهای داخلی و خارجی درآن؛
۷. ارتقای سطح دخالت و مشارکت مردم در بحث پدافند سایبری در فضای مجازی کشور؛
۸. پیشگیری و مقابله با تهدیدهای سایبری حاصل از توانمندی‌های انحصاری دشمن درفضای مجازی؛
۹. پیشگیری و مقابله با تهدیدهای عملیات روانی دشمن در فضای مجازی؛
۱۰. پیشگیری و مقابله با تهدیدهای فرهنگی، اقدامات ضد انقلابی و ضد دینی و فعالیتهای افراطی قومی- مذهبی در فضای مجازی.

یافته‌های تحقیق

۳۰ شاخصهٔ مذکور به دو پرسش کلی الف - ب و ۳۰ سؤال تبدیل شده و طی پرسشنامه‌ای بین ۲۰۵ نفر از صاحب‌نظران رشته‌های مرتبط دارای مدارک کارشناسی ارشد و دکترا توزیع شد که نتایج تجزیه و تحلیل آن به شرح ذیل است:

توزیع پاسخگویان به پرسش الف (به نظر شما آیا بسیج مردمی می‌تواند در پدافند سایبری نقش مؤثری داشته باشد؟)، نشان می‌دهد همهٔ پاسخ‌دهندگان، با پاسخ «بله» به تأثیرمتغیّر مستقل بر متغیّر میانی تحقیق تأکید دارند.

توزیع پاسخگویان به پرسش ب(به نظرشما آیا می‌توان با پدافند سایبری بر

امنیت ملی تأثیر گذاشت؟)، نشان می‌دهد همهٔ پاسخ‌دهندگان، با پاسخ «بله» به تأثیرمتغیّر مستقل به متغیّر میانی تحقیق تأکید دارند.

جدول ۱: شاخصه‌های ارائه شده و نتایج بیشترین فراوانی پاسخ هر یک از آنها در حجم نمونهٔ ۲۰۵ نفر

شاخص	پاسخ بیشترین فراوانی	درصد بیشترین فراوانی
۱. آیا در کشور ما، مراکز مناسب برای تربیت و آموزش نیروی انسانی ماهر به منظور دفاع در حوزهٔ سایبر وجود دارد؟	خیلی کم	۳۰،۲
۲. آیا سازمانهایی برای سازماندهی و به کارگیری افراد وفادار به نظام درحوزهٔ دفاع سایبر وجود دارند؟	متوسط	۲۸،۳
۳. آیا افراد داوطلب توانمند و وفادار به نظام در راستای پدافند سایبری کشور، وجود دارد؟	زیاد	۴۱
۴. حضور اعضای بسیج اقشار در پروژه‌های مربوط به پدافند و دفاع سایبری به چه میزان است؟	متوسط	۲۹،۳
۵. آیا شبکهٔ ارتباطی فعالان سایبری و فادار به نظام نظیر شبکه‌های اجتماعی مجازی و وب‌سایتها و پایگاههای ارتباطی میان اعضای بسیج مستضعفین وجود دارد؟	کم	۳۰،۷
۶. آیا قوانین مصوب و حمایت قضائی مناسبی از اقدامات فعالان همسو در راستای پدافند سایبری وجود دارد؟	کم	۲۷،۳
۷. آیا سازمانهای مردم‌نهاد طرفدار نظام که در فضای سایبر فعالیت می‌کنند، وجود دارند؟	خیلی کم	۲۸،۳
۸. آیا پروژه‌های عملیاتی شده توسط نهادهای انقلابی طرفدار نظام در راستای پدافند سایبری وجود داشته و انجام می‌شود؟	متوسط	۲۹،۸
۹.میزان حضور، آمادگی و فعالیت برخط و بهنگام شبکهٔ بسیج سایبری در اقدامات پدافند سایبری چقدراست؟	متوسط	۳۲،۷
۱۰. میزان پشتیبانی فنی، مالی، معنوی و حقوقی از فعالان و اعضای شبکهٔ عوامل و منابع سایبری را چقدر ارزیابی می‌کنید؟	خیلی کم	۲۸،۸
۱۱. آیا فنّاوری‌های بومی و ملّی در حوزهٔ سایبر (ضد بدافزار بومی، سیستم عاملهای بومی و...) وجود دارد؟	متوسط	۲۵،۹
۱۲. میزان دسترسی شبکهٔ عوامل و منابع و فعالان همسو به وبگاههای همسو را چقدر ارزیابی می‌کنید؟	متوسط	۲۹،۸
۱۳. کاهش ضریب بهره‌برداری از سایتهای فیلترشده و غیرمجاز و وبگاههای غیرهمسو چقدر انجام شده و توانمند است؟	متوسط	۳۷،۶
۱۴. به نظر شما میزان پروژه‌های سازمانهای دولتی در پدافند سایبری و امنیت ملی چقدراست؟	متوسط	۳۱،۷
۱۵. به نظر شما نسبت دانشجویان وفادار به نظام و بسیجی در رشته‌های سایبری به سایر دانشجویان در ایران چقدر است؟	متوسط	۲۹،۸

شاخص	پاسخ بیشترین فراوانی	درصد بیشترین فراوانی
۱۶. میزان عملیاتهای سایبری (هک وبگاه و...) در جهت مقابله و پیشگیری از اقدامات دشمن به نظر شما چقدر است؟	متوسط	۳۵,۶
۱۷. وجود هماهنگی و تعامل میان سازمانهای مرتبط با پدافند سایبری (نظامی، انتظامی، امنیتی و...) در ایران چقدر است؟	کم	۲۷,۳
۱۸.زیر ساختهای امن و مطمئن سایبری (فیبر نوری و...) به چه میزان در راستای پیشگیری و مقابله با تهدیدهای سایبری دشمن وجود دارد؟	متوسط	۳۱,۷
۱۹. اثر و فایده کنترل دسترسی به اینترنت در شرایط بحرانی برای مقابله با تهدیدهای سایبری دشمن چقدر است؟	خیلی زیاد	۲۸,۳
۲۰. به چه میزان در کشور مراکز اطلاع‌رسانی در راستای آگاه‌سازی مردم برای پدافند سایبری وجود دارد؟	کم	۳۸,۵
۲۱.امنیت سامانه‌های اساسی ملی و سامانه‌های فنّاوری اطلاعات و ارتباطات، در کشور به چه میزان است؟	متوسط	۳۴,۶
۲۲.امنیت بانکهای اطلاعاتی ملی و مراکز داده‌های امن، در کشور به چه میزان است؟	متوسط	۳۴,۶
۲۳.امنیت و حفاظت فیزیکی از زیرساختهای سایبری، در کشور به چه میزان است؟	متوسط	۳۳,۷
۲۴.سطح مقبولیت و مشروعیت نظام با استفاده از ظرفیت فضای مجازی، درکشور به چه میزان است؟	زیاد	۳۳,۲
۲۵. صحّت، سلامت و اعتماد در مدیریت اقتصاد ملی، بازار بورس و تجارت الکترونیک در فضای مجازی به چه میزان است؟	متوسط	۳۶,۱
۲۶. میزان اشراف نیروهای مسلّح و سازمانهای امنیتی بر فضای مجازی و رصد فعالیتهای داخلی و خارجی چقدر است؟	زیاد	۳۱,۲
۲۷. به نظر شما سطح دخالت و مشارکت مردم در پدافند سایبری، درفضای مجازی کشور به چه میزان است؟	متوسط	۲۸,۸
۲۸. پیشگیری و مقابله با تهدیدهای سایبری حاصل از توانمندی‌های انحصاری دشمن در فضای مجازی، به چه میزان است؟	متوسط	۴۱,۵
۲۹. پیشگیری و مقابله با تهدیدهای عملیات روانی دشمن در فضای مجازی، در کشور به چه میزان است؟	متوسط	۳۷,۱
۳۰. پیشگیری و مقابله با تهدیدهای فرهنگی، اقدامات ضدانقلابی و ضددینی در فضای مجازی، در کشور به چه میزان است؟	متوسط	۲۸,۳

برای آزمون نرمال بودن امتیاز متغیّرها از آزمون غیر پارامتری کولموگروف-اسمیرنوف[1] استفاده شد. این آزمون به عنوان یک آزمون تطابق توزیع برای داده‌های

1. Kolmogorov-Smirnov

کمّی است.هرگاه محقق نمونه‌ای از اندازه‌های کمّی دراختیار دارد و بخواهد تعیین کند که آیا این نمونه از جامعه‌ای با توزیع نرمال به دست آمده است یا خیر،از آزمون نرمال بودن یک توزیع بهره می‌جوید که یکی از شایع‌ترین آزمونها برای نمونه‌های کوچک است که محقق به نرمال بودن آن شک دارد.برای این هدف، آزمونK-S، آزمون مناسبی است(آموزش آمار، ۱۳۹۲). در این آزمون اگر معیار تصمیم[1]کمتر از ۵ درصد باشد، فرض صفر رد می‌شود؛ یعنی داده‌ها نمی‌توانند از یک توزیع خاص مانند نرمال، پواسن، نمایی یا یکنواخت باشند.فرضیهٔ صفر(H_0)در اینجا این است که:«تمایل خاصی در انتخاب گزینه‌ها وجود ندارد».

جدول ۲: نتایج آزمون کولموگروف-اسمیرنوف

آمارهای توصیفی								
گویه‌ها	N	میانگین	انحراف استاندارد	کمینه	بیشینه	درصدفراوانی		
						۲۵th	۵۰th (میانه)	۷۵th
آیا درکشورما، مراکز مناسبی جهت تربیت و آموزش نیروی انسانی ماهر به منظور دفاع سایبری وجود دارد؟	۲۰۵	۳.۲۶	۱.۴۰۶	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
آیا سازمانهایی، جهت سازماندهی و به کارگیری افراد وفادار به نظام درحوزه دفاع سایبر وجود دارند؟	۲۰۵	۳.۵۵	۱.۳۰۰	۱	۷	۳.۰۰	۳.۰۰	۴.۰۰
آیا افراد داوطلب توانمند و وفادار به نظام درراستای پدافند سایبری کشور، وجود دارد؟	۲۰۵	۴.۵۴	۱.۱۷۳	۱	۷	۴.۰۰	۵.۰۰	۵.۰۰
حضور اعضای بسیج اقشار درپروژه‌های مربوط به پدافند سایبری چه میزان است؟	۲۰۵	۳.۷۸	۱.۳۸۸	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
آیا شبکه ارتباطی فعالان سایبری و فادار به نظام، میان اعضای بسیج مستضعفین به طور مناسب وجود دارد؟	۲۰۵	۳.۳۵	۱.۴۵۹	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
آیا قوانین مصوب و حمایت قضائی مناسبی جهت حمایت ازاقدامات فعالان همسو برای پدافند سایبری وجود دارد؟	۲۰۵	۳.۶۵	۱.۸۷۷	۱	۷	۲.۰۰	۳.۰۰	۵.۰۰
آیا سازمانهای مردم نهاد طرفدار نظام که در فضای سایبر فعالیت نمایند، وجود و حضور دارند؟	۲۰۵	۳.۴۴	۱.۵۲۵	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
آیا پروژه‌های عملیاتی شده توسط نهادهای انقلابی طرفدار نظام درراستای پدافند سایبری انجام می‌شود؟	۲۰۵	۳.۸۳	۱.۴۲۵	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰

1. P-Value

آمارهای توصیفی								
گویه‌ها	N	میانگین	انحراف استاندارد	کمینه	بیشینه	درصدفراوانی		
						۲۵th	۵۰th (میانه)	۷۵th
میزان حضور، آمادگی و فعالیت برخط و به هنگام به شبکه بسیج سایبری در اقدامات پدافند سایبری چقدراست؟	۲۰۵	۳.۷۴	۱.۳۸۲	۱	۷	۳.۰۰	۴.۰۰	۴.۰۰
میزان پشتیبانی فنی، مالی، معنوی و حقوقی از فعالان واعضای شبکه عوامل و منابع سایبری را چقدر ارزیابی می‌کنید؟	۲۰۵	۳.۴۲	۱.۶۳۰	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
آیا فنّاوری‌های بومی و ملی درحوزه سایبر وجود دارد؟	۲۰۵	۳.۴۸	۱.۴۴۴	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
میزان دسترسی شبکه عوامل و منابع و فعالان همسو به وبگاههای همسو را چقدر ارزیابی می‌کنید؟	۲۰۵	۳.۹۶	۱.۴۴۶	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
کاهش ضریب بهره برداری از وب گاههای فیلترشده، غیرمجاز و غیرهمسو چقدر انجام شده و توانمند است؟	۲۰۵	۴.۱۲	۱.۲۷۹	۲	۷	۳.۰۰	۴.۰۰	۵.۰۰
به نظر شما میزان پروژه‌های سازمانهای دولتی درپدافند سایبری و امنیت ملی چقدراست؟	۲۰۵	۳.۷۳	۱.۳۶۵	۱	۷	۳.۰۰	۴.۰۰	۴.۰۰
به نظرشمانسبت دانشجویان وفاداربه نظام و بسیجی دررشته‌های سایبری به سایر دانشجویان درایران چقدر است؟	۲۰۵	۴.۰۱	۱.۲۷۲	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
میزان عملیاتهای سایبری درجهت مقابله و پیشگیری ازاقدامات دشمن به نظر شما چقدر است؟	۲۰۵	۴.۱۹	۱.۱۹۸	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
وجود هماهنگی وتعامل میان سازمانهای مرتبط با پدافند سایبری در ایران چقدر است؟	۲۰۵	۳.۸۱	۱.۴۶۰	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
زیر ساختهای امن ومطمئن سایبری و مدیریت مؤثر کمیت و کیفیت ارتباطات به چه میزان در راستای پیشگیری و مقابله با تهدیدهای سایبری دشمن وجود دارد؟	۲۰۵	۴.۰۱	۱.۳۴۱	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰
اثر و فایده کنترل دسترسی به اینترنت در شرایط بحرانی برای مقابله با تهدیدهای سایبری دشمن چقدر است؟	۲۰۵	۴.۷۰	۱.۳۳۴	۱	۷	۴.۰۰	۵.۰۰	۶.۰۰

آمارهای توصیفی								
گویه‌ها	N	میانگین	انحراف استاندارد	کمینه	بیشینه	درصدفراوانی		
						۲۵th	۵۰th (میانه)	۷۵th
به چه میزان در کشور مراکز اطلاع‌رسانی در راستای آگاه سازی مردم برای پدافند سایبری وجود دارد؟	۲۰۵	۳.۰۲	۱.۱۶۳	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
امنیت سامانه‌های اساسی ملی و سامانه‌های فنّاوری اطلاعات و ارتباطات، درکشور به چه میزان است؟	۲۰۵	۴.۳۵	۱.۲۶۹	۱	۷	۴.۰۰	۴.۰۰	۵.۰۰
امنیت بانک‌های اطلاعاتی ملی و مراکز داده‌های امن، درکشور به چه میزان است؟	۲۰۵	۴.۵۱	۱.۳۱۲	۲	۷	۴.۰۰	۴.۰۰	۵.۰۰
امنیت و حفاظت فیزیکی از زیرساختهای سایبری، درکشور به چه میزان است؟	۲۰۵	۴.۵۸	۱.۱۵۹	۲	۷	۴.۰۰	۵.۰۰	۵.۰۰
سطح مقبولیت و مشروعیت نظام با استفاده از ظرفیت فضای مجازی، درکشور به چه میزان است؟	۲۰۵	۴.۶۶	۱.۲۳۷	۲	۷	۴.۰۰	۵.۰۰	۵.۰۰
صحت، سلامت واعتماد در مدیریت اقتصاد ملی و بازار بورس و تجارت الکترونیک درفضای مجازی، به چه میزان است؟	۲۰۵	۴.۱۹	۱.۳۲۳	۲	۷	۳.۰۰	۴.۰۰	۵.۰۰
میزان اشراف نیروهای مسلّح و سازمانهای امنیتی بر فضای مجازی چقدر است؟	۲۰۵	۴.۵۶	۱.۱۶۰	۲	۷	۴.۰۰	۵.۰۰	۵.۰۰
به نظر شما سطح دخالت و مشارکت مردم در پدافندسایبری، درفضای مجازی کشور به چه میزان است؟	۲۰۵	۳.۴۱	۱.۲۳۶	۱	۷	۲.۰۰	۳.۰۰	۴.۰۰
مقابله با تهدیدهای سایبری حاصل از توانمندی‌های انحصاری دشمن در فضای مجازی، به چه میزان است؟	۲۰۵	۴.۲۰	۱.۲۲۶	۱	۷	۴.۰۰	۴.۰۰	۵.۰۰
مقابله با تهدیدهای عملیات روانی دشمن در فضای مجازی، درکشور به چه میزان است؟	۲۰۵	۳.۸۵	۱.۱۴۱	۱	۶	۳.۰۰	۴.۰۰	۵.۰۰
مقابله با تهدیدهای فرهنگی، اقدامات ضدانقلابی و ضددینی و درفضای مجازی، درکشور به چه میزان است؟	۲۰۵	۳.۷۳	۱.۲۸۱	۱	۷	۳.۰۰	۴.۰۰	۵.۰۰

در جدول ۲، مقادیر انحراف معیار استاندارد و میانگین بیان شده است. کمترین میانگین با ۳,۰۲ از آنِ این پرسش است که: «به چه میزان درکشورمراکزاطلاع‌رسانی درراستای آگاه‌سازی مردم برای پدافند سایبری وجوددارد؟». بیشترین میانگین را با مقدار ۴,۷، این پرسش دارد که: «اثر و فایدهٔ کنترل دسترسی به اینترنت در شرایط بحرانی برای مقابله با تهدیدهای سایبری دشمن چقدر است؟». کمترین انحراف استاندارد (۱,۱۴۱) مربوط به پرسش: «پیشگیری و مقابله با تهدیدهای عملیات روانی دشمن در فضای مجازی، درکشور به چه میزان است؟» و بیشترین انحراف استاندارد (۱,۸۷۷) مربوط به: «آیا قوانین مصوّب و حمایت قضایی مناسبی برای حمایت ازاقدامات فعالان همسو درراستای پدافند سایبری وجود دارد؟».

با توجه به اینکه انحراف استاندارد، بیانگر پراکندگی و تغییرپذیری نمره‌هاست و هر چه بزرگ باشد، تغییرپذیری آنها بیشتر و برعکس، هر چه کمتر باشد، تغییرپذیری یا پراکندگی کمتر است(حافظنیا، ۱۳۸۹:۱۲۷). با این حساب، کمترین تغییرپذیری و پراکندگی مربوط به شاخص «مقابله با تهدیدهای عملیات روانی دشمن» بوده و بیشترین تغییرپذیری و پراکندگی را شاخص «وجود قوانین مصوّب و حمایت قضایی مناسب ازاقدامات فعالان همسو درراستای پدافند سایبری» دارد؛ یعنی نظر پاسخ‌دهندگان به شاخص «مقابله با تهدیدهای عملیات روانی دشمن» خیلی نزدیک به هم است، ولی پاسخ‌دهندگان نسبت به شاخص «وجود قوانین مصوّب و حمایت قضایی مناسب ازاقدامات فعالان همسو درراستای پدافند سایبری»، نظرات پراکنده‌ای دارند.

همبستگی بین شاخصها

آیا همبستگی معناداری بین این گویه‌ها وجود دارد یا خیر؟ تحلیل همبستگی آماری ابزاری است برای تعیین نوع و درجهٔ رابطهٔ یک متغیّر با متغیّر کمّی دیگر. ضریب همبستگی، شدت رابطه و همچنین نوع رابطه را نشان می‌دهد. در صورتی که فرض نرمال بودن داده‌ها معقول نباشد، از ضریب همبستگی اسپیرمن[1] استفاده می‌شود.

فرمول همبستگی اسپیرمن (الگوریتم جدول‌بندی متقاطع[2]):

1. Spearman Correlation
2.Crosstabulations Algorithms

جدول ۳: نتایج آزمون همبستگی (غیرپارامتری)اسپیرمن برای شاخصهای بسیج مردمی

			مراکز تربیت و آموزش	مراکز سازماندهی افراد	افراد داوطلب توانمند	پروژه‌های بسیج اقشار	شبکه بسیج سایبری	قوانین وحمایت قضایی	سمن‌ها	پروژه‌های نهادهای انقلابی	حضور برخط شبکه سایبری	پشتیبانی فنی ومالی
ضریب همبستگی اسپیرمن	مراکز تربیت و آموزش	ضریب همبستگی۱	1.000	.565**	.170*	.302**	.241**	.100	.214**	.106	.163*	.204**
		Sig.(دوطرفه)	.	.000	.015	.000	.001	.153	.002	.129	.020	.003
		N	205	205	205	205	205	205	205	205	205	205
	مراکز سازماندهی افراد	ضریب همبستگی	.565**	1.000	.270**	.407**	.281**	.227**	.289**	.243**	.295**	.309**
		Sig.(دوطرفه)	.000	.	.000	.000	.000	.001	.000	.000	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	افراد داوطلب توانمند	ضریب همبستگی	.170*	.270**	1.000	.221**	.169*	.031	.123	.130	.222**	.026
		Sig.(دوطرفه)	.015	.000	.	.001	.016	.655	.078	.063	.001	.707
		N	205	205	205	205	205	205	205	205	205	205
	پروژه‌های بسیج اقشار	ضریب همبستگی	.302**	.407**	.221**	1.000	.414**	.253**	.215**	.222**	.373**	.350**
		Sig.(دوطرفه)	.000	.000	.001	.	.000	.000	.002	.001	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	شبکه بسیج سایبری	ضریب همبستگی	.241**	.281**	.169*	.414**	1.000	.363**	.346**	.230**	.346**	.400**
		Sig.(دوطرفه)	.001	.000	.016	.000	.	.000	.000	.001	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	قوانین وحمایت قضایی	ضریب همبستگی	.100	.227**	.031	.253**	.363**	1.000	.235**	.343**	.339**	.476**
		Sig.(دوطرفه)	.153	.001	.655	.000	.000	.	.001	.000	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	سمن ها	ضریب همبستگی	.214**	.289**	.123	.215**	.346**	.235**	1.000	.348**	.394**	.314**
		Sig.(دوطرفه)	.002	.000	.078	.002	.000	.000	.	.000	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	پروژه‌های نهادهای انقلابی	ضریب همبستگی	.106	.243**	.130	.222**	.230**	.343**	.348**	1.000	.486**	.311**
		Sig.(دوطرفه)	.129	.000	.063	.001	.001	.000	.000	.	.000	.000
		N	205	205	205	205	205	205	205	205	205	205
	حضور آنلاین شبکه سایبری	ضریب همبستگی	.163*	.295**	.222**	.373**	.346**	.339**	.394**	.486**	1.000	.436**
		Sig.(دوطرفه)	.020	.000	.001	.000	.000	.000	.000	.000	.	.000
		N	205	205	205	205	205	205	205	205	205	205
	پشتیبانی فنی و مالی	ضریب همبستگی	.204**	.309**	.026	.350**	.400**	.476**	.314**	.311**	.436**	1.000
		Sig.(دوطرفه)	.003	.000	.707	.000	.000	.000	.000	.000	.000	.
		N	205	205	205	205	205	205	205	205	205	205

*: همبستگی معنادار وقابل توجه درسطح ۰/۰۵ (دوطرفه).

**: همبستگی معنادار وقابل توجه درسطح ۰/۰۱ (دوطرفه).

مقادیر ذکر شده بزرگ‌تر از ۰/۰۵ نشان می‌دهند که بین دو متغیّر«مراکز تربیت و آموزش، قوانین و حمایت قضایی» و بین دو متغیّر«افراد داوطلب توانمند» با «قوانین و حمایت قضایی» و دو متغیّر «افراد داوطلب توانمند» با «پشتیبانی فنی و مالی» و دو متغیّر«افراد داوطلب توانمند» با «پروژه‌های نهادهای انقلابی»، همبستگی وجود ندارد. در این جدول، مقدار sig حاصل از تقاطع شاخص «میزان پشتیبانی فنی و مالی از فعالان پدافند سایبری» با شاخص «وجود افراد داوطلب توانمند در حوزهٔ دفاع سایبری» عدد ۰/۷۰۷ بوده و بزرگ‌تر از ۰/۰۵ است؛ یعنی این دو شاخص، همبستگی ندارند. همچنین شاخص «وجود افراد داوطلب توانمند در حوزهٔ دفاع سایبری» با شاخص «قوانین وحمایت قضایی» (sig=۰/۶۵۵) و با شاخص «سمن‌ها[۱]» (sig=۰/۰۷۸) و «پروژه‌های نهادهای انقلابی» (sig =۰/۰۶۳) و «پشتیبانی فنی ومالی» (sig =۰/۷۰۷) همبستگی ندارد؛ ولی با سایر شاخصها همبستگی دارد(sig<۰/۰۵). شاخص «مراکز تربیت و آموزش» با شاخصهای «قوانین وحمایت قضایی» (مقدار sigبرابربا ۰/۱۵۳) و شاخص «پروژه‌های نهادهای انقلابی» (sig =۰/۱۲۹)، همبستگی ندارد. مقدار sig برای دو شاخص «پروژه‌های نهادهای انقلابی» و «افراد داوطلب توانمند» برابر است با ۰/۰۶۳و چون بزرگ‌تر از ۰/۰۵ است، نشان می‌دهد این دو شاخص، همبستگی ندارند. گفتنی است شاخصهای «مراکز سازماندهی افراد»، «پروژه‌های بسیج اقشار» و «شبکهٔ بسیج سایبری»، با تمام شاخصهای متغیّر بسیج مردمی همبستگی دارند.

با توجه به آزمونهای آماری، تجزیه و تحلیل داده‌ها، نظر کارشناسان، مصاحبه‌ها و مشاهدات محقق، یافته‌های تحقیق و راهکارهای ارائه شده شامل موارد زیر است:

نیاز به افزایش مراکز علمی و آموزشی در خصوص پدافند سایبری و گنجاندن دروس آشنایی با تهدیدهای سایبری و پدافند سایبری در دانشگاهها و مدارس، به خصوص آموزش بسیجیان.

نیاز به افزایش و تعریف پروژه‌های مناسب و کاربردی در سازمانهای دولتی و نهادهای انقلابی طرفدار نظام و رده‌های بسیج اقشار، نظیر بسیج مهندسان، بسیج دانشجویی و... در راستای پدافند سایبری و افزایش بهره‌گیری از توان آنها در پروژه‌های سایبری کشور.

ایجاد و افزایش سازمانهایی برای سازماندهی و به کارگیری افراد وفادار به نظام در حوزهٔ دفاع سایبر نظیر توسعهٔ پایگاههای مقاومت بسیج و تشکّلهای فرهنگی مساجد در راستای پدافند سایبری.

۱. سازمان های مردم نهاد (NGO)

بهبود روشهای جذب و به کارگیری داوطلبان توانمند و وفادار به نظام در استای پدافند سایبری.

افزایش کیفیت وکمّیت شبکه‌های اجتماعی مجازی سالم و مناسب و توسعهٔ آن برای ارتباط فعالان سایبری وفادار به نظام و افزایش پایگاههای ارتباطی اعضای بسیج مستضعفین و تشکیل شبکهٔ بسیج سایبری.

اعمال سیاستها و تدابیر و برنامه‌هایِ تشویقی و حمایتیِ مالی و معنوی نسبت به اعضای شبکهٔ بسیج سایبری، در خصوص افزایش حضور و آمادگی و برخط[1] بودن در مواقع نیاز به اقدامات پدافندی و عملیات روانی و....

اعمال سیاستها و تدابیری برای افزایش تولیدات داخلی فنی و سایبری و حمایت از تولیدکنندگان فنّاوری‌های بومی و ملی در حوزهٔ سایبر.

تدبیر و برنامه‌ریزی برای طراحی سامانه‌های ارتباطی شبکه‌های عوامل و منابع پنهان و آشکار در فضای مجازی به صورت نرم‌افزاری و سخت‌افزاری، به منظور ارتباط جهت اطلاع‌رسانی و ارسال اخبار در اسرع وقت به رده‌های بالاتر (با مدّ نظر قرار دادن حفاظت، قدرت، سرعت و امنیت ارتباطات).

اصلاح روشهای فیلترینگ سایتهای غیرمجاز و افزایش کارایی و ثبات این روشها با توجه به پیشرفتهای سریع این حوزه و افزایش تأثیرپذیری اعمال فیلترینگ وبگاههای غیر مجاز. با توجه به تولید روزانه هزاران وبگاه که تعدادی زیادی از آنها علیه امنیت جامعه می‌باشند، لزوم ورود بسیج مردمی برای مقابله با آنها احساس می‌شود.

نیاز به تعریف و طراحی چارچوب مشخص برای انجام عملیات سایبری توسط افراد و گروهها و سازمانها و نیاز به برنامه‌ریزی مناسب و اعمال تدابیر هماهنگ‌کننده در خصوص انجام عملیات سایبری هک و نفوذ و مقابله با وبگاههای دشمن در فضای مجازی، که توسط اقدامگران داخلی صورت می‌گیرد؛ زیرا گاهی، اقدامات تاکتیکی برخی نیروهای وفادار به نظام، موجب خلل در اقدامات راهبردی حکومت می‌شود و گاهی اقدامات آنها خارج از چارچوب ضوابط دیپلماتیک و بر ضد منافع و مصالح ملی است. برای مثال، افرادی بر اساس احساساتِ زودگذر و موردی، اقدام به هک سایتهای دولتی یا مردمی کشورهای بیگانه می‌کنندکه معمولاً این امر به نام دولت ایران ثبت می‌شود؛ در حالی که با توجه به ضعف برنامه‌ای و ساختاری این نوع حملات سایبری بر خلاف منافع کشوراست.

افزایش تأثیر و فعالیت و عضویت سازمان بسیج مستضعفین در شورای عالی فضای مجازی کشور.

1. On Line

برنامه‌ریزی راهبردی و بلندمدت در خصوص کاهش دخالت توانمندی‌های انحصاری دشمن در فضای مجازی و افزایش توانمندی‌های داخلی در این امر، به خصوص تلاش برای بومی‌سازی فنّاوری‌های فضای مجازی از قبیل سیستم‌های عامل، زیرساخت، نرم‌افزارها و سخت‌افزارهای امنیت سایبری و....

به کارگیری کارشناسان و متخصصان دارای تعهد بالای اخلاقی و اعتقادی در امورات فنی و سایبری و پشتیبانی زیرساختها و شبکه‌ها و بانکهای اطلاعاتی مهم و اساسی کشور.

برنامه‌ریزی و اعمال سیاستها و تدابیر و آمادگی برای کنترل دسترسی به اینترنت و فضای مجازی در شرایط بحرانی برای مقابله با عوامل بیگانه و تهدیدهای سایبری و عوامل ناآگاه داخلی که در این شرایط، اقدامات ضد امنیت ملی را انجام می‌دهند؛ نظیر اقداماتی که در سال ۱۳۸۸ پس از انتخابات ریاست جمهوری دهم روی داد و افراد و گروههایی بر ضد منافع ملی به شایعه‌پراکنی و دروغ‌پردازی و و عملیات روانی پرداختند.

برنامه‌ریزی و اتخاذ سیاستها و تدابیر حمایتی برای افزایش مراکز اطلاع‌رسانی در راستای آگاه‌سازی مردم در امر پدافند سایبری و بهره‌گیری بیشتر از توان بسیج مردمی.

آموزش شبکه‌های اطلاعات بسیج در خصوص جمع‌آوری اطلاعات سایبری و روشهای فنی اطلاع‌رسانی آن به حاکمیت جهت افزایش رصد اقدامات مجرمانهٔ افراد و گروهها، در فضای مجازی در خصوص تجارت الکترونیک و برخورد قانونی با شبکه‌های هرمی و مقابله با گسترش فساد اقتصادی از طریق فضای مجازی و برنامه‌ریزی در راستای افزایش سلامت و امنیت تجارت الکترونیک کشور.

برنامه‌ریزی و اتخاذ تدابیری در خصوص افزایش اشرافیت سازمان بسیج مستضعفین، نیروهای مسلّح و سازمانهای امنیتی و انتظامی بر فضای مجازی.

اعمال تدابیر و سیاستها و برنامه‌ریزی در خصوص مقابله با عملیات روانی دشمن و مقابله با تهدیدهای فرهنگی و اقدامات ضد انقلابی و ضد دینی دشمن در فضای مجازی و حمایتهای مالی و معنوی از سازمانها و گروههایی که اقدام به راه‌اندازی وبگاهها و انجام اقدامات مقابله‌ای با عملیات روانی دشمن و مقابله با تهدیدهای فرهنگی و اقدامات ضد انقلابی و ضد دینی دشمن در فضای مجازی انجام می‌دهند.

با توجه به تهدیدها و فرصتهای جدید فضای مجازی و رشد روز افزوون فنّاوری اطلاعات و ارتباطات، نیاز به بروزرسانی، دانسته‌ها و اطلاعات مسئولان لشکری و کشوری در مقاطع زمانی منظم و برنامه‌ریزی شده وجود دارد.

پیشنهاد ایجاد جایگاه «مدیریت سایبری» برای رده‌های بسیج، حتی تا سطح پایگاه مقاومت بسیج که می‌تواند شرح وظایفی مشابه موارد ذیل داشته باشد:

الف) اطلاع‌رسانی جرایم رایانه‌ای برای مقابله با آنها توسط سازمانهای مربوط؛

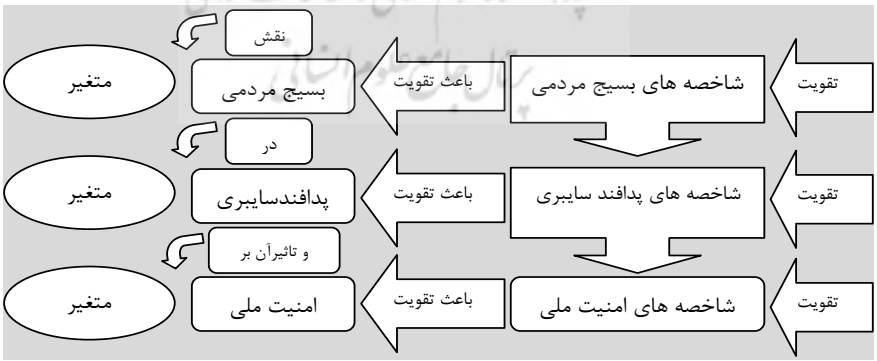
ب) سازماندهی افراد داوطلب و توانمند به انجام هک و نفوذ و عملیات سایبری و معرفی به زیر مجموعه‌های فرماندهی فضای مجازی سپاه در استانها؛

ج) رصد و اخذ ارسال اخبار امنیتی مربوط به فضای مجازی و اینترنت و شبکه‌های ماهواره‌ای، به سازمانهای مربوط؛

د) شناسایی موردی تهدیدهای سایبری بسته به کار تخصصی هر رده و گزارش به ردهٔ بالاتر؛

نتیجه‌گیری

با دقت در مراحل انجام پژوهش و با مدّ نظر قرار دادن تأثیر و تاثّر متقابل شاخصه‌های تحقیق برهم و تأثیرات متغیّر مستقل بسیج مردمی(به عنوان نقش) بر متغیّر میانی پدافند سایبری و تأثیرات متغیّر میانی بر متغیّر وابستهٔ امنیت ملی،همچنین نظر متخصصان و تجزیه و تحلیل داده‌ها، گویای آن است که از طریق تقویت شاخصه‌های بسیج مردمی، می‌توان بر پدافند سایبری تأثیر گذاشت و آن را تقویت کرد. همچنین از طریق تقویت شاخصه‌های پدافند سایبری می‌توان باعث ارتقای سطح امنیت ملی کشور شد؛ تأثیرات در جهت عکس مراحل مربوط، باعث تضعیف پدافند سایبری و کاهش سطح امنیت ملی می‌شود.



شکل۲- بسیج مردمی در پدافند سایبری نقش داشته و آن هم بر امنیت ملی تاثیر دارد.

با توجه به شاخصه‌های ارائه شده؛ افزایش توان بسیج مردمی، قدرت ملی را افزایش می‌دهد که به نوبهٔ خود، توان دفاع به ویژه در بُعد پدافند سایبری افزایش خواهد یافت و این افزایش توان پدافند سایبری، موجب ارتقای سطح امنیت ملی خواهد شد. در نظرگرفتن نقش بسیج مردمی و آفندوپدافندسایبری، جزءجدایی‌ناپذیراز ابعاد امنیت ملی وروابط خارجی و بین‌المللی امروزی دراکثرکشورهای رقیب و درگیر و متخاصم است که خواسته یاناخواسته،گریزی ازآن نیست وبایدهرچه سریع‌تر،جامع‌تر،توانمندتر و آماده‌تردراین میدان واردشد؛ زیرا ارتقای سطح امنیت ملی و حتی فراملی (برای چنددولت متحدیا ائتلافی)، همواره در برنامه‌ریزی‌های راهبردی دولتهامدّ نظرقرار می‌گیرد. با توجه به موارد مطرح شده، مسئولان و مدیران، بایستی برای نقش بسیج مردمی اهمیت بیشتری قایل شده، برای توانمندسازی بسیج مردمی در راستای پدافند سایبری، اقدامات مناسبِ عنوان شده در یافته‌های تحقیق را مدّ نظر قرار دهند تا شاهد ارتقای سطح امنیت ملی جمهوری اسلامی ایران باشیم.

منابع

۱. آربسکلاو، مایکل(۱۳۸۷)؛**جنگ اطلاعات: چگونه ازحملات سایبری درامان باشیم،** ترجمه علی ناصری و عبدالمجید ریاضی، تهران، دانشگاه عالی دفاع ملی.

۲. آنجلیز، جینا دی.(۱۳۸۳)، **جرایم سایبر،** ترجمه سعید حافظی و عبدالصمد خرم‌آبادی، تهران، شورای عالی اطلاع‌رسانی ریاست جمهوری.

۳. آیکاو، دیوید جی. و همکاران(۱۳۸۳)؛**راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای،** ترجمه اکبر استرکی وهمکاران، [بی‌جا]، [بی‌نا].

۴. بشیری، عباس(۱۳۸۸)؛**بررسی امنیت از تئوری تا عمل،** تهران،[بی‌جا].

۵. بوزمان، آدا برومر(۱۳۸۲)؛**اطلاعات استراتژیک وکشورداری،** ترجمه پژوهشکدهٔ مطالعات راهبردی، تهران، پژوهشکدهٔ مطالعات راهبردی.

۶. بونی، ویلیام سی. و جرالد ال.کواسیج(۱۳۸۳)؛**جاسوسی شبکه‌ای: تهدیدجهانی اطلاعات،** ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران، دانشکده امام باقر(ع).

۷. بیات، غلامرضا(۱۳۹۱)؛**«آفند و پدافند سایبری، برای پایداری امنیت ملی»،** امنیت پایدار، جلد دوم، تهران، دانشگاه جامع امام حسین(ع).

۸. بیات، غلامرضا(۱۳۹۲)؛**نقش بسیج مردمی در پدافند سایبری و تأثیر آن بر امنیت ملی ج.ا.ایران،** پایان‌نامه کارشناسی ارشد اطلاعات استراتژیک، تهران، دانشگاه جامع امام حسین(ع).

۹. پاینده، ابوالقاسم(۱۳۸۵)؛**نهج‌الفصاحه،** اصفهان، خاتم‌الانبیا.

۱۰.حافظ نیا، محمدرضا(۱۳۸۹)؛**مقدمه‌ای برروش تحقیق درعلوم انسانی،** تهران، سمت.

۱۱.حسن‌بیگی، ابراهیم(۱۳۸۳)؛**«توسعهٔشبکهٔ ملی دیتا، چالشهای فرارو و تهدیدهای متوجه امنیت ملی»،** مجله اندیشه انقلاب اسلامی، ش ۹: ۱۲۷-۷۶.

۱۲.حسن‌بیگی، ابراهیم(۱۳۸۴)؛**حقوق وامنیت درفضای سایبر،** تهران، ابرارمعاصر.

۱۳.دانشگاه امام حسین(ع)(۱۳۷۶)؛**اصول و مبانی استراتژی،** تهران، دانشگاه امام حسین(ع).

۱۴.رابینز، کوین و فرانک وبستر(۱۳۸۴)؛**عصرفرهنگ فنّاورانه: ازجامعهٔ اطلاعاتی تازندگی مجازی،** ترجمه مهدی داودی، تهران، توسعه.

۱۵.روحی، نبی الله(۱۳۹۱)؛ **«نظریه امنیت مردمی در جمهوری اسلامی ایران»،** چکیده مقالات همایش سراسری امنیت پایدار، تهران، دانشگاه جامع اما حسین(ع).

۱۶.سید مفیدی، کاوه(۱۳۸۳)؛**جنگ سایبری،** تهران، [بی‌نا].

۱۷.صالحی امیری، رضا و همکاران(۱۳۸۷)؛**مدیریت بحران رسانه،** تهران، مرکز تحقیقات استراتژیک مجمع تشخیص مصلحت نظام.

۱۸.ضیائی‌پرور، حمید(۱۳۸۳)؛**جنگ نرم: ویژهٔ جنگ رایانه‌ای،** جلد ۱، تهران، ابرار معاصر.

۱۹.ضیائی‌پرور، حمید(۱۳۸۷)؛**«ساماندهی وبلاگها و وبسایتها»**، مجموعه مقالات تکنولوژی‌های جدید رسانه‌ای، تهران، مرکز تحقیقات استراتژیک مجمع تشخیص مصلحت نظام.
۲۰.عباسی، مهدی و تورج هاشمی(۱۳۸۹)؛**«نقش رسانه‌ای اینترنت در ناهنجاری‌های اجتماعی در فضای سایبری در میدان جنگ نرم»**، ماهنامه مهندسی فرهنگی، سال پنجم، ش ۵۰-۴۹ (بهمن و اسفند): ۶۳-۵۵.
۲۱.عبدالله‌خانی، علی(۱۳۸۹)؛**نظریه‌های امنیت**، تهران، ابرار معاصر.
۲۲.عبداللهی، علی(۱۳۹۰)؛**«امنیت یکی از مؤلفه‌های اقتدار ملی است»**:
http://mellatonline.net
۲۳.کارازوجیانی، آتینا(۱۳۸۸)؛**سیاستهای منازعهٔ سایبری**، ترجمه محبوبه بیات، تهران، مرکزپژوهشی شهیدصیاد شیرازی.
۲۴.کرونین، اُدری کورت(۱۳۸۵)؛**«بسیج اینترنتی، شیوهٔ نوین جذب نیروهای مردمی»**، فصلنامه مطالعات راهبردی بسیج، سال نهم، ش۳۳: ۷۳-۸۷.
۲۵.کلهر، رضا(۱۳۸۶)؛**«بسیج و تکنولوژی اطلاعات»**، فصلنامه مطالعات راهبردی بسیج، سال دهم، ش۱۹:۳۶-۵.
۲۶.کیوان حسینی، اصغر(۱۳۸۱)؛**«تبیین اصول و فرمول دفاع همه‌جانبه از دیدگاه امام خمینی(ره) با تأکید بر نقش بسیج»**، فصلنامه مطالعات راهبردی بسیج، ش۱۶: ۱۳۶-۱۲۵.
۲۷.لیبیکی، مارتین(۱۳۸۴)؛**جنگ سایبری**، تهران، وزارت دفاع و پشتیبانی نیروهای مسلّح.
۲۸.مرادی، حجت‌اله(۱۳۸۹)؛**عملیات روانی و رسانه**، تهران، ساقی، چ دوم.
۲۹.مرکز توزیع پیام دیدار(۱۳۹۱)؛**آوردگاهی مجازی برای جنگی حقیقی**، تهران، مرکز توزیع پیام دیدار.
۳۰.مطهرنیا، مهدی(۱۳۷۶)؛**«بسیج و نقش آن در دفاع همه‌جانبه»**، فصلنامه مطالعات راهبردی بسیج، ش۱۵: ۴۲-۲۶.
۳۱.مورگنتا،هانس جی(۱۳۸۹)؛**سیاست میان ملتها**، ترجمه حمیرا مشیرزاده، تهران، وزارت امور خارجه.
۳۲.نای، جوزف(۱۳۹۰)؛**قدرت سایبری**، هاروارد، مرکزعلوم وامور بین‌الملل بلفر.
۳۳.نای، جوزف(۱۳۸۷)؛**قدرت نرم**، ترجمه سیدمحسن روحانی و مهدی ذولفقاری، تهران، دانشگاه امام صادق(ع).
۳۴.نقیب‌السادات، سیدرضا(۱۳۸۹)؛**«تهدیدهای رسانه‌ای غرب و نقش بسیج در رفع تهدیدها»**، فصلنامه مطالعات راهبردی بسیج، سال سیزدهم، ش۱۱۹:۴۸-۸۳.
۳۵.توکلی(۱۳۹۱): http://urban-management.persianblog.ir

۳۶.عراقی(۱۳۹۱): http://www.tebyannews.com
۳۷.گرداب(۱۳۹۲)؛ وبگاه مرکز بررسی جرائم سازمان‌یافتهٔ سایبری سپاه پاسداران انقلاب اسلامی: http://www.gerdab.ir
۳۸.وبگاه امام خمینی(ره)(۱۳۹۲): http://www.Imam-khomeini.ir
۳۹.وبگاه تریپ وایر(۱۳۹۲): http://www.tripwire.com
۴۰.وبگاه خبر آلاین(۱۳۹۱): http://www.khabaronline.ir
۴۱.وبگاه دانشنامهٔ آزاد ویکی‌پدیا(۱۳۹۲): http://fa.wikipedia.org

42. Ashton, Catherine (2013).**Remarks by EU High Representative at Press Conference on the Launch of the EU's Cyber Security Strategy**, Brussels: eeas, Europa, eu.
43. Ashton, Catherine (2013).**The Launch of the EU's Cyber Security Strategy**, Brussels: eeas, Europa, eu.
44. Europa.eu (2013).**EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity**, Georgia Tech Information Security Center.
45. Europa.eu (2013).**Proposed Directive on Network and Information Security**,Brussels: Europa, eu.
46. Lee, Wenke & Bo Rotoloni (2013).**"Emerging Cyber Threat,Georgia: Georgia Institute of Technology"**: *gtcyberSecuritySummit.com.*
47. Libicki, Martin (2009).**Cyber Deterrence and Cyber Warfare**: www.rand.org.
48. Maa Ben,Hans Georg (2013).**Verfassungsschutz-Präsident Sieht Gefahr der Cyber-Mobilization**, Berlin: www.heise-medien.de.
49. Odierno, Raymond T.& John M. McHugh (2013).**Army Strategic Planning Guidance. United States**, United States Army Chief of Staff.
50. Shimeall,Timothy & Phil Williams (2011). **Countering Cyber War**, (none).
51. Sommer, Peter & Brown, Lan (2011), **Reducing Systemic Cybersecurity Risk**, Information Systems and Innovation Group, France (oecd.org): International Futures Programme OECD.
52. The European Commission (2013).**EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity**,Brussels, The European Commission.

53. Thomas,Timothy L. (2013).**Cyber Mobilizition: A Growing Counterinsurgency Campaign**, Foreign Military Studies Office (Army) Fort Leaven Worth KS, www.stormingmedia.us.
54. Thuraisingham, Bhavani &Jan Kallberg (2013).**Cyber Operations, Bridging from Concept to Cyber Superiority**, (none).
55. Wilshusen,Gregory C. (2013). **Cyber Security.**
56. Laer,Jeroen VanandPeter Van Aelst(2012).**"Cyber-Protest and Civil Society"**,*the Internet and Action Repertoires in Social Movements*, Capture 12, P.230-254.
57. PASW Statistics18 (2013).SPSS Help:www.spss.com: PASW Statistics.